Lecture Notes in Mathematics 1467

Wolfgang M. Schmidt

Diophantine Approximations and Diophantine Equations

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Author

Wolfgang M. Schmidt
Department of Mathematics, University of Colorado
Boulder, Colorado, 80309-0426, USA

Mathematics Subject Classification (1991): 11J68, 11J69, 11O57, 11D61

ISBN 3-540-54058-X Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-54058-X Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2146/3140-543210 - Printed on acid-free paper

Preface

The present notes are the outcome of lectures I gave at Columbia University in the fall of 1987, and at the University of Colorado 1988/1989. Although there is necessarily some overlap with my earlier Lecture Notes on Diophantine Approximation (Springer Lecture Notes 785, 1980), this overlap is small. In general, whereas in the earlier Notes I gave a systematic exposition with all the proofs, the present notes present a varirety of topics, and sometimes quote from the literature wihtout giving proofs. Nevertheless, I believe that the pace is again leisurely.

Chapter I contains a fairly thorough discussion of Siegel's Lemma and of heights. Chapter II is devoted to Roth's Theorem. Rather than Roth's Lemma, I use a generalization of Dyson's Lemma as given by Esnault and Viehweg. A proof of this generalized lemma is not given; it is beyond the scope of the present notes. An advantage of the lemma is that it leads to new bounds on the number of exceptional approximations in Roth's Theorem, as given recently by Bombieri and Van der Poorten. These bounds turn out to be best possible in some sense. Chapter III deals with the Thue equation. Among the recent developments are bounds by Bombieri and author on the number of solutions of such equations, and by Mueller and the author on the number of solutions of Thue equations with few nonzero coefficients, say s such coefficients (apart from the constant term). I give a proof of the former, but deal with the latter only up to $s = 3$, i.e., to trinomial Thue equations. Chapter IV is about S-unit equations and hyperelliptic equations. S-unit equations include equations such as $2^x + 3^y = 4^z$. I present Evertse's remarkable bounds for such equations. As for elliptic and hyperelliptic equations, I mention a few basic facts, often without proofs, and proceed to counting the number of solutions as in recent works of Evertse, and of Silverman, where the connection with the Mordell–Weil rank is explored. Chapter V is on certain diophantine equations in more than two variables. A tool here is my Subspace Theorem, of which I quote several versions, but without proofs. I study generalized S-unit equations, such as, e.g. $\pm a_1^{x_1} \pm a_2^{x_2} \pm \cdots \pm a_n^{x_n} = 0$ with given integers $a_i > 1$, as well as norm form equations. Recent advances permit to give explicit estimates on the number of solutions. The notes end with an Epilogue on the abc-conjecture of Oesterlé and Masser.

Hand written notes of my lectures were taken at Columbia University by Mr. Agboola, and at the University of Colorado by Ms. Deanna Caveny. The manuscript was typed by Ms. Andrea Hennessy and Ms. Elizabeth Stimmel. My thanks are due to them.

January 1991 Wolfgang M. Schmidt

Table of Contents

Table of Contents (cont.)

I. Siegel's Lemma and Heights

§1. Siegel's Lemma.

Consider a system of homogeneous linear equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned} \tag{1.1}$$

If $m < n$ and the coefficients lie in a field, then there is a nontrivial solution with components in the field. If $m < n$ and the coefficients lie in $\mathbb{Z}$ (the integers), then there is a nontrivial solution in integers. (Just take a solution with rational components and multiply by the common denominator.) It is reasonable to believe that if the coefficients are small integers, then there will also be a solution in small integers. This idea was used by A. Thue (1909) and formalized by Siegel in (1929; on p. 213 of his Collected Works).

LEMMA 1. *Suppose that in (1.1) the coefficients a_{ij} lie in $\mathbb{Z}$ and have $|a_{ij}| \leqq A$ $(1 \leqq i, j \leqq n)$ where A is natural. Then there is a nontrivial solution in $\mathbb{Z}$ with*

$$|x_i| < 1 + (nA)^{m/(n-m)} \qquad (i = 1, \dots, n).$$

Proof. We follow Siegel. Let H be an integer parameter to be specified later. Let C be the cube consisting of points

$$\underline{\underline{x}} = (x_1, \dots, x_n)$$

with

$$|x_i| \leqq H \qquad (i = 1, \dots, n).$$

There are $(2H+1)^n$ integer points in this cube, since there are $2H+1$ possibilities for each coordinate. Let T be the linear map $\mathbb{R}^n \to \mathbb{R}^m$ with

$$T\underline{\underline{x}} = (a_{11}x_1 + \cdots + a_{1n}x_n, \dots, a_{m1}x_1 + \cdots + a_{mn}x_n).$$

Writing $T\underline{\underline{x}} = \underline{\underline{y}} = (y_1, \dots, y_m)$, we observe that the image of C lies in the cube

$$C' : \quad |y_j| \leqq nAH \quad (j = 1, \dots, m)$$

of $\mathbb{R}^m$. The number of integer points in C' is $(2nAH+1)^m$. Suppose now that

$$(2nAH+1)^m < (2H+1)^n. \tag{1.2}$$

Then T restricted to the integers in the original cube will not be one-to-one. So there exist $\underline{\underline{x}}', \underline{\underline{x}}''$ in C, with $\underline{\underline{x}}' \neq \underline{\underline{x}}''$, such that $T\underline{\underline{x}}' = T\underline{\underline{x}}''$. Put $\underline{\underline{x}} = \underline{\underline{x}}' - \underline{\underline{x}}''$. Then $T\underline{\underline{x}} = \underline{\underline{0}}$. So $\underline{\underline{x}}$ is a solution to the system with integer coordinates. Note that $|x_i| \leqq 2H$ $(i =$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

$1,\dots,n$), because $|x_i'|, |x_i''| \leqq H$ $(i = 1,\dots,n)$, so $|x_i| = |x_i' - x_i''| \leqq |x_i'| + |x_i''| \leqq 2H$. Choose H to be the natural number satisfying

$$(nA)^{m/(n-m)} - 1 \leqq 2H < (nA)^{m/(n-m)} + 1.$$

Then

$$\begin{aligned}(2H+1)^n &= (2H+1)^m(2H+1)^{n-m}\\ &> (2H+1)^m(nA)^m\\ &> (2nAH+1)^m.\end{aligned}$$

So there exists an $\underline{\underline{x}}$ satisfying $|x_i| \leqq 2H < 1 + (nA)^{m/(n-m)}$.

So the proof of Siegel's Lemma uses the box principle.

Can the exponent be improved? The answer is "no".

Siegel's Lemma is almost best possible. Put $k = n - m$, and for large P pick distinct primes p_{ij} $(i \leqq i \leqq k, 1 \leqq j \leqq m)$ with $P\eta < p_{ij} < P$, where $0 < \eta < 1$ is given. Put

$$P_j = p_{1j}p_{2j}\cdots p_{kj} \quad (1 \leqq j \leqq m), \qquad P_{ij} = P_j/p_{ij} \quad (1 \leqq i \leqq k,\ 1 \leqq j \leqq m),$$

$$Q_i = p_{i1}p_{i2}\cdots p_{im} \quad (1 \leqq i \leqq k), \qquad Q_{ij} = Q_i/p_{ij} \quad (1 \leqq i \leqq k,\ 1 \leqq j \leqq m).$$

Consider the system of m equations in n variables:

$$\begin{array}{llll} P_{11}x_1 + \cdots + P_{k1}x_k - P_1y_1 & & & = 0\\ P_{12}x_1 + \cdots + P_{k2}x_k & -P_2y_2 & & = 0\\ \vdots & & & \\ P_{1m}x_1 + \cdots + P_{km}x_k & & -P_my_m & = 0.\end{array}$$

The maximum modulus A of its coefficients has $A \leqq P^k$. The following are solution vectors:

$$\begin{aligned}\underline{\underline{z}}_1 &= (Q_1, 0, \dots, 0, Q_{11}, Q_{12}, \dots, Q_{1m})\\ &\vdots\\ \underline{\underline{z}}_k &= (0, 0, \dots, Q_k, Q_{k1}, Q_{k2}, \dots, Q_{km}).\end{aligned}$$

It is clear that every solution of our system of equations is a linear combination $c_1\underline{\underline{z}}_1 + \cdots + c_k\underline{\underline{z}}_k$. For integer solutions, c_i is necessarily a rational number whose denominator is Q_i, and then every component of $c_i\underline{\underline{z}}_i$ has denominator Q_i. Moreover, if, say, c_1 is not integral, then (since $Q_{11}, Q_{12}, \dots, Q_{1m}$ are coprime), $c_1\underline{\underline{z}}_1$ is not integral and has some component whose denominator is a prime p_{1j}. But since $c_2\underline{\underline{z}}_2, \dots, c_k\underline{\underline{z}}_k$ don't have p_{1j} in the denominator, $c_1\underline{\underline{z}}_1 + c_2\underline{\underline{z}}_2 + \cdots + c_k\underline{\underline{z}}_k$ cannot be integral—a contradiction. Therefore the integer solutions are $\underline{\underline{z}} = c_1\underline{\underline{z}}_1 + \cdots + c_k\underline{\underline{z}}_k$ with $c_1, \dots, c_k$ in $\mathbb{Z}$. When $\underline{\underline{z}} \neq \underline{\underline{0}}$, say $c_1 \neq 0$, the first component x_1 of $\underline{\underline{z}}$ has

$$|x_1| \geqq Q_1 > (\eta P)^m = \eta^m P^m > \eta^m A^{m/k} = \eta^m A^{m/(n-m)}.$$

Therefore every integer solution $(x_1, \dots, x_k,\ y_1, \dots, y_m) \neq (0, \dots, 0)$ has

$$\max(|x_1|, \dots, |x_k|) > \eta^m A^{m/(n-m)}.$$

Here η may be taken arbitrarily close to 1.

Another approach is as follows. When $m = n-1$, consider the system of equations

$$Ax_i - x_{i+1} = 0 \qquad (i = 1, \dots, n-1).$$

Every nontrivial solution, in fact every nontrivial complex solution, has $x_n/x_1 = A^{n-1}$. Thus if we set

$$q(\underline{\underline{x}}) = \max |x_i/x_j|,$$

with the maximum over i, j in $1 \leqq i,\ j \leqq n$ with $x_j \neq 0$, then $q(\underline{\underline{x}}) = A^{n-1} = A^{m/(n-m)}$. But then for integer solutions, $\max(|x_1|, \dots, |x_n|) \geqq A^{m/(n-m)}$.

Exercise 1a. Suppose now that $m = 1$. For large A, construct an equation

$$a_1 x_1 + \cdots + a_n x_n = 0$$

with integral coefficients and $|a_i| \leqq A$ $(i = 1, \dots, n)$, such that every nontrivial solution $\underline{\underline{x}}$ with complex components has

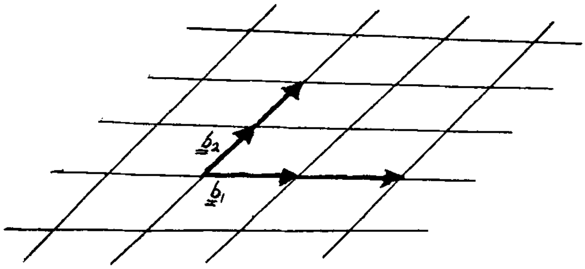
$$q(\underline{\underline{x}}) \geqq c(n) A^{1/(n-1)} = c_1(n,m) A^{m/(n-m)} > 0.$$

This approach can be carried out for general n, m. See Schmidt (1985).

§2. Geometry of Numbers.

The subject was founded by Minkowski (1896 & 1910). Other references are Cassels (1959), Gruber and Lekkerkerker (1987), and Schmidt (1980, Chapter IV).

A *lattice* Λ is a subgroup of $\mathbb{R}^n$ which is generated by n linearly independent vectors $\underline{\underline{b}}_1, \dots, \underline{\underline{b}}_n$ (linearly independent over $\mathbb{R}^n$). The elements of this lattice are $c_1 \underline{\underline{b}}_1 + \cdots + c_n \underline{\underline{b}}_n$ with $c_i \in \mathbb{Z}$.



The set $\underline{\underline{b}}_1, \dots, \underline{\underline{b}}_n$ is called a *basis*. A basis is not uniquely determined. For example, $\underline{\underline{b}}_1, \underline{\underline{b}}_1 + \underline{\underline{b}}_2, \underline{\underline{b}}_3, \dots, \underline{\underline{b}}_n$ is another basis.

How unique is a basis? Suppose $\underline{\underline{b}}'_1, \dots, \underline{\underline{b}}'_n$ is another basis. Then

$$\underline{\underline{b}}'_i = \sum_{j=1}^{n} c_{ij} \underline{\underline{b}}_j \quad \text{and} \quad c_{ij} \in \mathbb{Z}$$

and

$$\underline{b}_j = \sum_{i=1}^{n} c'_{ij}\underline{b}_i \quad \text{and} \quad c'_{ji} \in \mathbb{Z}.$$

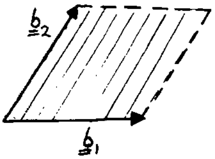
So the matrices (c_{ij}) and (c'_{ji}) are inverse to each other and $c_{ij}, c'_{ji} \in \mathbb{Z}$, so $\det(c_{ij}) = \det(c'_{ji}) = \pm 1$. Thus the matrix (c_{ij}) is *unimodular*, where by definition a unimodular matrix is a square matrix with integer entries and determinant 1 or -1.

LEMMA 2A. *A necessary and sufficient condition for a subset Λ of $\mathbb{R}^n$ to be a lattice is the following:*

(i) *Λ is a group under addition.*
(ii) *Λ contains n linearly independent vectors.*
(iii) *Λ is discrete.*

For a proof, see e.g., Schmidt (1980, Ch. IV, Theorem 8A).

Consider $\mathbb{R}^n$ with the Euclidean metric and Λ a lattice with $\underline{b}_1, \ldots, \underline{b}_n$ as basis. Let Π be the set of linear combinations $\lambda_1\underline{b}_1 + \cdots + \lambda_n\underline{b}_n$ with $0 \leqq \lambda_i < 1$ $(i = 1, \ldots, n)$. Then Π is called a *fundamental parallelepiped* of Λ.



The fundamental parallelepiped does depend on which basis is chosen. The volume of Π is given by $V(\Pi) = |\det(\underline{b}_1, \ldots, \underline{b}_n)|$ where the right-hand side involves the matrix whose rows are respectively made up of the coordinates of $\underline{b}_1, \ldots, \underline{b}_n$ with respect to an orthonormal bases of $\mathbb{R}^n$. This volume is independent of the chosen basis of the lattice, since different bases are connected by unimodular transformations. It is an invariant of the lattice.

We define

$$\det \Lambda = V(\Pi).$$

Notice that when $\underline{b}_i = (b_{i1}, \ldots, b_{in})$, then

$$V^2 = \det\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & & & \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \cdot \det\begin{pmatrix} b_{11} & b_{21} & \cdots & b_{n1} \\ b_{12} & b_{22} & \cdots & b_{n2} \\ \vdots & & & \\ b_{1n} & b_{2n} & \cdots & b_{nn} \end{pmatrix}$$

$$= \det\begin{pmatrix} \underline{b}_1\underline{b}_1 & \underline{b}_1\underline{b}_2 & \cdots & \underline{b}_1\underline{b}_n \\ \underline{b}_2\underline{b}_1 & \underline{b}_2\underline{b}_2 & \cdots & \underline{b}_2\underline{b}_n \\ \vdots & & & \\ \underline{b}_n\underline{b}_1 & \underline{b}_n\underline{b}_2 & \cdots & \underline{b}_n\underline{b}_n \end{pmatrix}, \tag{2.1}$$

where the inner product of vectors $\underline{x}$, $\underline{y}$ is denoted by $\underline{x}\,\underline{y}$.

Every $\underline{\underline{x}}$ in $\mathbb{R}^n$ may uniquely be written as $\underline{\underline{x}} = \underline{\underline{x}}' + \underline{\underline{x}}''$ where $\underline{\underline{x}}' \in \Pi$ and $\underline{\underline{x}}'' \in \Lambda$.

$$\underline{\underline{x}} = \sum_{i=1}^{n} \xi_i \underline{\underline{b}}_i = \underbrace{\sum_{i=1}^{n} \{\xi_i\} \underline{\underline{b}}_i}_{\in \Pi} + \underbrace{\sum_{i=1}^{n} [\xi_i] \underline{\underline{b}}_i}_{\in \Lambda} .$$

Here we used the notation that uniquely

$$\xi = [\xi] + \{\xi\}$$

where $[\xi]$ is an integer, called the *integer part* of ξ, and $\{\xi\}$ satisfies $0 \le \{\xi\} < 1$ and is called the *fractional part* of ξ.

$\mathbb{Z}^n$ is a lattice with basis $\underline{\underline{e}}_1, \dots, \underline{\underline{e}}_n$ where $\underline{\underline{e}}_i = (\overbrace{0, \dots, 0, 1}^{i}, 0, \dots, 0)$, $(i = 1, \dots, n)$, and with $\det \mathbb{Z}^n = 1$. If Λ is an arbitrary lattice with basis $\underline{\underline{b}}_1, \dots, \underline{\underline{b}}_n$, then there exists a linear transformation T such that $T\underline{\underline{e}}_i = \underline{\underline{b}}_i$ $(i = 1, \dots, n)$. So $T\mathbb{Z}^n = \Lambda$.

Is T unique? Suppose $T\mathbb{Z}^n = T'\mathbb{Z}^n$. Then $(T')^{-1}T\mathbb{Z}^n = \mathbb{Z}^n$, so $\det((T')^{-1}T) = \pm 1$ and $(T')^{-1}T$ is unimodular. Call it U. Then $T = T'U$. Observe that

$$\det \Lambda = |\det T|.$$

THEOREM 2B. (Minkowski's First Theorem on Convex Sets.) *Let $B \subseteq \mathbb{R}^n$ be a convex set which is symmetric about the origin (i.e., $\underline{\underline{x}} \in B$ if and only if $-\underline{\underline{x}} \in B$) of volume*

$$V(B) > 2^n \det \Lambda \tag{2.2}$$

where Λ is a lattice. Then B contains a non-zero lattice point.

Comments. The volume here is the Jordan volume, i.e., the Riemann integral over the characteristic function of the set. Every bounded convex set has such a volume. Let $\underline{\underline{g}} \in B$ be a non-zero lattice point in B. Then $-\underline{\underline{g}} \neq \underline{\underline{0}}$ and $-\underline{\underline{g}} \in B$ by symmetry, so B contains actually at least two non-zero lattice points.

Proof. (Mordell, 1934). $V(B)/\det \Lambda$ is invariant under non-singular linear maps. Therefore, after applying a linear transformation, we may assume that $\Lambda = \mathbb{Z}^n$. Then the theorem reduces to: *If $V(B) > 2^n$, then B contains a non-zero integer point.* Let B_m be the set of rational points in B with common denominator m. Then

$$\frac{|B_m|}{m^n} \longrightarrow V(B) \quad \text{as} \quad m \to \infty$$

where $|\ |$ denotes the cardinality. For m sufficiently large, $|B_m|/m^n > 2^n$ and thus $|B_m| > (2m)^n$. So there are two points $\underline{\underline{a}} = (a_1/m, \dots, a_n/m)$, $\underline{\underline{b}} = (b_1/m, \dots, b_n/m)$ in B_m with

$$a_i \equiv b_i \pmod{2m} \qquad (i = 1, \dots, n).$$

Then

$$\frac{1}{2}(\underline{\underline{a}} - \underline{\underline{b}}) \in B$$

since the midpoint of $\underline{a}$ and $-\underline{b}$ is $\frac{1}{2}(\underline{a}-\underline{b}) \in B$. Let $\underline{g} = \frac{1}{2}(\underline{a}-\underline{b})$. Clearly $\underline{g}$ is a non-zero integer point.

Exercise 2a. If B is symmetric, convex, and $V(B) > 2^n k \det \Lambda$ where $k \in \mathbb{N}$, then B contains at least k pairs of non-zero lattice points.

A *convex body* is a compact, convex set containing $\underline{0}$ as an interior point. Such a body clearly has $0 < V(B) < \infty$.

Remark 2C. If B is a symmetric, convex body and $V(B) \geqq 2^n \det \Lambda$, then B contains a non-zero lattice point. It is easy to show that 2C follows from 2B, and vice versa.

Remark 2D. Theorem 2B is best possible. Take $\Lambda = \mathbb{Z}^n$, B the cube with $|x_i| < 1$, $(i = 1, \dots, n)$. Then $V(B) = 2^n = 2^n \det \Lambda$ and there are no non-zero integer points in B.

Minkowski defines *successive minima* as follows: Given B, Λ where B is symmetric, convex, bounded, and with $\underline{0}$ in its interior, let $\lambda_1 = \inf\{\lambda : \lambda B$ contains a non-zero lattice point$\}$. * More generally, for $1 \leqq j \leqq n$, $\lambda_j = \inf\{\lambda : \lambda B$ contains j linearly independent lattice points$\}$. Then

$$0 < \lambda_1 \leqq \lambda_2 \leqq \lambda_3 \leqq \cdots \leqq \lambda_n < \infty.$$

Here $\lambda_1 > 0$ since B is bounded and $\lambda_n < \infty$ since $\underline{0}$ is an interior point.

THEOREM 2E. (Minkowski's Second Theorem on Convex Bodies.)

$$\frac{2^n}{n!} \det \Lambda \leqq \lambda_1 \cdots \lambda_n V(B) \leqq 2^n \det \Lambda. \tag{2.3}$$

Example. Let $n = 2$, $\Lambda = \mathbb{Z}^2$ and B the rectangle $|x_1| \leqq k$, $|x_2| \leqq 1/k$ where $k \geqq 1$. Then $\lambda_1 = 1/k$, $\lambda_2 = k$ and $\lambda_1 \lambda_2 V(B) = V(B) = 4 = 2^2 \det \Lambda$.

A proof will not be given here. There is no really simple proof of the upper bound in (2.3). A weaker bound is proved in Schmidt (1980, p. 88).

Remark 2F. The constants $2^n/n!$ and 2^n are best possible. Let $\Lambda = \mathbb{Z}^n$ and B the cube $|x_i| \leqq 1$. Then $V(B) = 2^n$. Now $\underline{e}_1, \dots, \underline{e}_n$ are on the boundary, so $\lambda_1 = \cdots = \lambda_n = 1$. We have $\lambda_1 \cdots \lambda_n V(B) = 2^n$ and $2^n \det \Lambda = 2^n$. So we get equality on the right-hand side of (2.3). Next, let $\Lambda = \mathbb{Z}^n$ and B the "octahedron" $|x_1| + \cdots + |x_n| \leqq 1$. It may be seen that $V(B) = 2^n/n!$. We have again $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$. Thus $(2^n/n!) \det \Lambda = 2^n/n!$ and $\lambda_1 \cdots \lambda_n V(B) = 2^n/n!$. We have equality on the left-hand side of (2.3).

Note that

$$\lambda_1^n V(B) \leqq 2^n \det \Lambda \tag{2.4}$$

*λB is the set of points $\lambda \underline{x}$ with $\underline{x} \in B$.

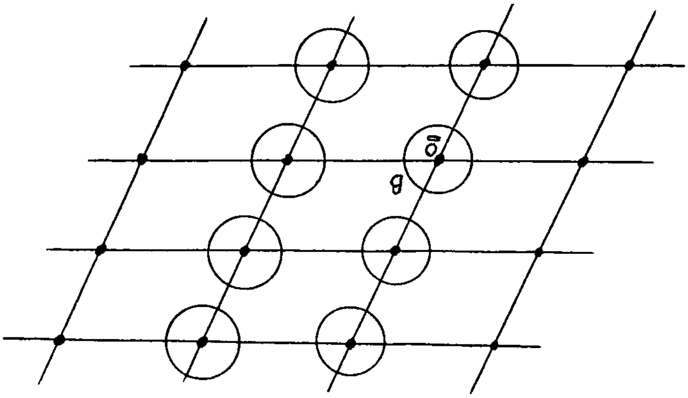
since $\lambda_1 \leqq \lambda_2 \leqq \cdots \leqq \lambda_n$. Suppose now that $V(B) > 2^n \det \Lambda$. Then $\lambda_1 < 1$ so that $B = 1B \supset \lambda_1 B$ contains a non-zero lattice point. Therefore (2.4) implies $2B$. It is easily seen that (2.4) and $2B$ are equivalent.

Exercise 2b. Suppose B is a symmetric, convex set, Λ a lattice, λ_1 the first minimum. Given $\mu > 0$, the number of lattice points in μB is $\leqq ((2\mu/\lambda_1) + 1)^n$.

§3. Lattice Packings.

A good reference for general packing and covering problems is C. A. Rogers (1964).

Let $B \subset \mathbb{R}^n$ be compact and measurable. Given a lattice Λ, write $B + \Lambda = \{\underline{\underline{b}} + \underline{\underline{\ell}} : \underline{\underline{b}} \in B,\ \underline{\underline{\ell}} \in \Lambda\}$.



If the translates of B by vectors of Λ are disjoint (as in the picture), then we call $B + \Lambda$ a *lattice packing* of B. Having disjoint translates is equivalent to having unique representations of the vectors of $B + \Lambda$ as $\underline{\underline{b}} + \underline{\underline{\ell}}$.

The *density* of such a lattice packing is

$$\delta(B, \Lambda) = \lim_{r \to 0} \frac{V(\Lambda + B, r)}{V(r)} \tag{3.1}$$

where $V(r)$ is the volume of a ball of radius r, and $V(\Lambda + B, r)$ is the volume of the intersection of $\Lambda + B$ with the ball of radius r and center $\underline{\underline{0}}$.

Exercise 3a. Show that the limit (3.1) always exists under our hypotheses, and that (with Π a fundamental parallelepiped)

$$\delta(B, \Lambda) = V(\Pi \cap (\Lambda + B))/V(\Pi) = V(B)/\det \Lambda.$$

We define

$$\delta(B) = \sup_{\substack{\Lambda \\ \Lambda + B \text{ a lattice} \\ \text{packing}}} \delta(B, \Lambda).$$

This is invariant under nonsingular linear transformations T, since $\delta(TB, T\Lambda) = \delta(B, \Lambda)$.

Suppose B is convex and symmetric about $\underline{\underline{0}}$. Suppose B contains no non-zero lattice point.

Claim: Then $\Lambda + \frac{1}{2}B$ is a lattice packing.

Justification: Suppose $\underline{\underline{\ell}}_1 + \frac{1}{2}\underline{\underline{b}}_1 = \underline{\underline{\ell}}_2 + \frac{1}{2}\underline{\underline{b}}_2$ where $\underline{\underline{\ell}}_1$, $\underline{\underline{\ell}}_2 \in \Lambda$, $\underline{\underline{b}}_1$, $\underline{\underline{b}}_2 \in B$. Then by an argument used above, $\frac{1}{2}\underline{\underline{b}}_1 - \frac{1}{2}\underline{\underline{b}}_2$ is in $B \cap \Lambda$. But $\frac{1}{2}\underline{\underline{b}}_1 - \frac{1}{2}\underline{\underline{b}}_2 = \underline{\underline{\ell}}_2 - \underline{\underline{\ell}}_1$ and B contains no non-zero lattice points, so that $\underline{\underline{\ell}}_2 - \underline{\underline{\ell}}_1 = \underline{\underline{0}}$, $\underline{\underline{\ell}}_2 = \underline{\underline{\ell}}_1$, hence $\underline{\underline{b}}_1 = \underline{\underline{b}}_2$. Therefore $\Lambda + \frac{1}{2}B$ is indeed a lattice packing.

$$\delta(\frac{1}{2}B, \Lambda) = \frac{V(\frac{1}{2}B)}{\det \Lambda} = \frac{V(B)}{2^n \det \Lambda} \leqq \delta\left(\frac{1}{2}B\right) = \delta(B) \leqq 1$$

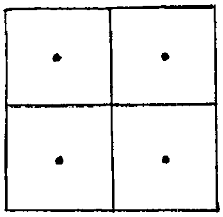
and therefore

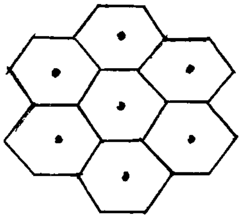
$$V(B) \leqq 2^n \delta(B) \det \Lambda.$$

THEOREM 3A. *If B is convex and symmetric about $\underline{\underline{0}}$ and $V(B) > 2^n \delta(B) \det \Lambda$, then B contains a non-zero lattice point.*

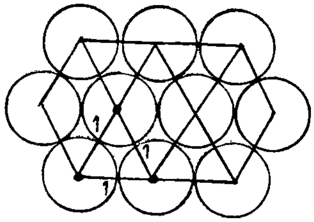
In particular, this happens when $V(B) > 2^n \det \Lambda$. So 3A is a strengthening of Minkowski's Theorem 2B.

Remark 3B. For B convex, symmetric about $\underline{\underline{0}}$, one can show that $\delta(B) < 1$ except for certain polyhedra. E.g., the cube has density $\delta = 1$. So do regular hexagons in the plane.





Let $\delta_n = \delta(B)$ where B is a ball in $\mathbb{R}^n$. Consider the following picture.



The "triangle" lattice Λ has $\det \Lambda = \frac{1}{2}\sqrt{3}$. It is easy to guess that

$$\delta_2 = \frac{V(B)}{\det \Lambda} = \frac{(\frac{1}{2})^2 \pi}{\frac{1}{2}\sqrt{3}}.$$

This had already been proved implicitly by Gauss in his theory of positive definite binary quadratic forms. We know the values of $\delta_2, \delta_3, \ldots, \delta_8$; see Cassels (1959, Appendix) and Exercise 3b below. The estimation of δ_n for large n remains among the central unsolved problems in the Geometry of Numbers. Blichfeldt (1929) proved that $\delta_n \leqq 2^{-n/2}(1+\frac{n}{2})$. Also, $\delta_n \geqq (\frac{1}{2} - \varepsilon)^n$ if $n > n_0(\varepsilon)$. See Cassels (1959, p. 249). More recently, G.A. Kabatjanskii and V.I. Levenšteĭn (1978) have shown that $\delta_n \leqq 2^{-0.599n(1-\epsilon)}$ for $n > n_0(\epsilon)$.

One may in a fairly obvious way define a general (not necessarily lattice) packing of a set B, and the maximum general packing density. For a disk in $\mathbb{R}^2$, Thue (1892) had shown that the maximum packing density is in fact achieved for a lattice–packing. It is not known whether a similar result holds for a ball in $\mathbb{R}^3$. It is generally believed that the densest packing density of a ball in $\mathbb{R}^n$ where n is sufficiently large is less than the smallest lattice packing density.

Now $V(B)\lambda_1^n \leqq 2^n \det \Lambda \delta(B)$, so that $\lambda_1 \leqq 2(\det \Lambda)^{1/n}(\delta(B)/V(B))^{1/n}$. For the unit ball B, $V(B) = V(n) = \pi^{n/2}/\Gamma(1+\frac{n}{2})$, so that by Stirling's formula we have the asymptotic relation

$$V(n)^{2/n} = V(B)^{2/n} \sim \frac{2\pi e}{n} \quad \text{as} \quad n \to \infty.$$

We define *Hermite's constant* γ_n to be least such that for any lattice Λ

$$\lambda_1 \leqq \gamma_n^{1/2}(\det \Lambda)^{1/n}$$

where $\lambda_1 = \lambda_1$ (unit ball). So

$$\gamma_n \leqq \frac{4\delta_n^{2/n}}{V(n)^{2/n}} \leqq \frac{2n}{\pi} \qquad \text{if} \quad n \geq 2.$$

We have $\overline{\lim}(\gamma_n/n) \leqq \frac{4}{2\pi e} = \frac{2}{\pi e}$, by using the trivial estimate $\delta_n \leqq 1$. If instead we use Blichfeldt's estimate, we obtain $\overline{\lim}(\gamma_n/n) \leqq \frac{1}{\pi e}$. The result of Kabatjanskii and Levenšteĭn quoted above yields $\overline{\lim}(\gamma_n/n) \leqq 2^{-0.197}(\pi e)^{-1}$.

Exercise 3b. Show that $\gamma_n = 4\delta_n^{2/n}/V(n)^{2/n}$.

Exercise 3c. Let $Q(\underline{\underline{X}}) = \sum_{i,j=1}^n a_{ij}X_iX_j$ be a positive definite quadratic form with real coefficients $a_{ij} = a_{ji}$. Then there exists a non-zero integer point $\underline{\underline{x}}$ with $Q(\underline{\underline{x}}) \leqq \gamma_n(\det Q)^{1/n}$. Moreover, γ_n is least with this property.

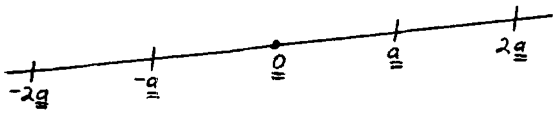
§4. Siegel's Lemma Again.

A *rational subspace* of $\mathbb{R}^n$ or $\mathbb{C}^n$ is a subspace spanned by vectors with rational coordinates. A rational subspace S^k of dimension k is spanned by k vectors $\underline{\underline{a}}_1, \ldots, \underline{\underline{a}}_k \in \mathbb{Q}^n$. Such a space S^k may be defined by $n-k$ linear homogeneous equations with rational coefficients. The integer points in a subspace S^k form a set Λ which is a lattice of S^k by Lemma 2A.

The *height* of S^k is defined by

$$H(S^k) = \det \Lambda.$$

An integer point $\underline{\underline{a}} = (a_1, \dots, a_n)$ is called *primitive* if $gcd(a_1, \dots, a_n) = 1$. Then $\underline{\underline{a}}$ is "closest to the origin," i.e., there is no integer point on the line segment between $\underline{\underline{0}}$ and $\underline{\underline{a}}$. Either $\underline{\underline{a}}$ or $-\underline{\underline{a}}$ is a basis of the 1-dimensional lattice of integer points of the space S^1 spanned by $\underline{\underline{a}}$. Thus $H(S^1) = |\underline{\underline{a}}|$.



By the definition of Hermite's constant, there is on S^k an integer point $\underline{\underline{x}} \neq \underline{\underline{0}}$ with

$$|\underline{\underline{x}}| \leqq \gamma_k^{1/2} H(S^k)^{1/k}.$$

LEMMA 4A. *Consider the unit cube C in $\mathbb{R}^n$, i.e., $|x_i| \leqq 1$ $(i = 1, \dots, n)$. Let S^k be a k-dimensional subspace. Then $C \cap S^k$ has k-dimensional volume $\geqq 2^k$.*

This result, due to J. Vaaler (1979), will not be proved here.

Let S^k be a rational subspace, Λ the lattice of integer points associated with S^k, i.e., $\Lambda = \Lambda(S^k)$. Let $B = C \cap S^k$. By Minkowski's Theorem 2C, $\lambda_1^k V(B) \leqq 2^k \det \Lambda$. Now $V(B) \geqq 2^k$ so that

$$\lambda_1^k 2^k \leqq 2^k \det \Lambda,$$
$$\lambda_1^k \leqq \det \Lambda = H(S^k),$$
$$\lambda_1 \leqq H(S^k)^{1/k}.$$

Recall that $|\underline{\underline{x}}|$ was the Euclidean norm. Let

$$\overline{|\underline{\underline{x}}|} = \max(|x_1|, \dots, |x_n|)$$

be the maximum norm. Our results may be summarized in

LEMMA 4B. *Given a rational subspace S^k there is an integer point $\underline{\underline{x}} \neq \underline{\underline{0}}$ on S^k with*

$$|\underline{\underline{x}}| \leqq \gamma_k^{1/2} H(S)^{1/k}.$$

Also, there is such a point $\underline{\underline{x}}^1$ with

$$\overline{|\underline{\underline{x}}^1|} \leqq H(S)^{1/k}.$$

When S^k is a rational subspace, then $(S^k)^\perp$ is a rational subspace of dimension $m = n - k$.

LEMMA 4C. $H(S^\perp) = H(S)$.

The proof is postponed to the next section (see Corollary 5J). To make the lemma correct for S^0 and $S^n = \mathbb{R}^n$, we set $H(S^0) = 1$.

Let us go back to a system of linear equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

where $0 < m < n$, $a_{ij} \in \mathbb{Z}$. If these equations are independent, they define a rational subspace S^k of dimension $k = n - m$. And $(S^k)^\perp$ is spanned by the row vectors $\underline{\underline{a}}_1, \ldots, \underline{\underline{a}}_m$ where $\underline{\underline{a}}_i = (a_{i1}, \ldots, a_{in})$. Then

$$H(S^k) = H(S^{k\perp}) \leqq |\underline{\underline{a}}_1| \cdots |\underline{\underline{a}}_m|.$$

The last inequality occurs because $\underline{\underline{a}}_1, \ldots, \underline{\underline{a}}_m$ can be written as linear combinations of basis vectors for the lattice, so that $\det|\underline{\underline{a}}_1, \ldots, \underline{\underline{a}}_m|$ is an integer multiple of the determinant of a basis.‡ Thus

$$\det(\Lambda(S^{k\perp})) \leqq |\det(\underline{\underline{a}}_1, \ldots, \underline{\underline{a}}_m)| \leqq |\underline{\underline{a}}_1| \cdots |\underline{\underline{a}}_m|$$

by Hadamard's inequality, which is a consequence of Lemma 5E below.

LEMMA 4D. (Siegel's Lemma) *Given the system of equations above,*

(i) *there is a non-trivial integer solution* $\underline{\underline{x}}$ *with*

$$|\underline{\underline{x}}| \leqq \gamma_{n-m}^{1/2}(|\underline{\underline{a}}_1| \cdots |\underline{\underline{a}}_m|)^{1/(n-m)} \leqq \left(\frac{2}{\pi}n\right)^{1/2} (\sqrt{n}\,A)^{m/(n-m)}$$

if $|a_{ij}| \leqq A$ *for every* i, j.

(ii) *Also, there is a non-trivial integer solution* $\underline{\underline{x}}^1$ *with*

$$\overline{|\underline{\underline{x}}^1|} \leqq (|\underline{\underline{a}}_1| \cdots |\underline{\underline{a}}_m|)^{1/(n-m)} \leqq (\sqrt{n}\,A)^{m/(n-m)}.$$

In the first inequality we used that $\gamma_{n-m} < \frac{2}{\pi}(n-m) < \frac{2}{\pi}n$ if $n - m \geqq 2$, and $\gamma_{n-m} = 1 < \frac{2}{\pi}n$ if $n - m = 1$, so that $n \geqq 2$. It is clear that we do not have to restrict to the case when the m equations are independent.

Remark 4E. If Minkowski's Second Theorem (2E) is used, (ii) can be strengthened to get the following: *there are* $n - m$ *linearly independent solutions* $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_{n-m}$ *of our system of equations such that*

$$\overline{|\underline{\underline{x}}_1||\underline{\underline{x}}_2|} \cdots \overline{|\underline{\underline{x}}_{n-m}|} \leqq |\underline{\underline{a}}_1| \cdots |\underline{\underline{a}}_m|.$$

The first assertion can be strengthened in the same way, but this is not so obvious.

§5. Grassman Algebra.

‡We think of $\underline{\underline{a}}_1, \ldots, \underline{\underline{a}}_m$ as vectors with m components in terms of an orthonormal coordinate system in $S^{k\perp}$

(Also presented in Schmidt (1980), Ch. IV.) Notation: Let K be a field, K^n a vector space, and $\underline{\underline{e}}_i = (\underbrace{0,\dots,0,1}_{i},0,\dots,0)$ be basis vectors. Suppose $0 \leqq p \leqq n$. Let $C(n,p)$ be the set of p–tuples $\sigma = \{i_1,\dots,i_p\}$ with $i_j \in \mathbb{Z}$ and $1 \leqq i_1 < i_2 < \cdots < i_p \leqq n$. This set has cardinality

$$|C(n,p)| = \binom{n}{p}.$$

Let $\underline{\underline{E}}_\sigma$ be the formal expression

$$\underline{\underline{E}}_\sigma = \underline{\underline{e}}_{i_1} \wedge \underline{\underline{e}}_{i_2} \wedge \cdots \wedge \underline{\underline{e}}_{i_p}.$$

There are $\binom{n}{p}$ such expressions. For $p = 0$, let $\underline{\underline{E}}_\phi = 1$. Let K^n_p be the vector space over K generated by $\underline{\underline{E}}_\sigma$ with $\sigma \in C(n,p)$. Then $\dim(K^n_p) = \binom{n}{p}$. Elements of K^n_p are called *p–vectors.*

Special cases: $K^n_1 = K^n$, $K^n_0 = K$, and K^n_n is spanned by the single vector $\underline{\underline{e}}_1 \wedge \underline{\underline{e}}_2 \wedge \cdots \wedge \underline{\underline{e}}_n$.

We now introduce a more flexible notation. For any p and any integers $i_1,\dots,i_p$ between 1 and n, the symbol $\underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p}$ should be $\underline{\underline{0}}$ if $i_j = i_{j'}$ for some $j \neq j'$. Otherwise, if $\{i_1,\dots,i_p\} = \{j_1,\dots,j_p\}$, (considered as unordered sets), where $j_1 < j_2 < \cdots < j_p$, then

$$\underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p} = \pm \underline{\underline{e}}_{j_1} \wedge \cdots \wedge \underline{\underline{e}}_{j_p}$$

with the $+$ sign if we get the i's from the j's by an even permutation, and with the $-$ sign otherwise.

Set

$$G_n = K^n_0 \oplus K^n_1 \oplus \cdots \oplus K^n_n.$$

Then $\dim G_n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.

We are going to make G_n into an algebra over K. We need a product, or wedge $\wedge$. By linearity, it suffices to define products of the basis vectors $\underline{\underline{E}}_\sigma$. We set

$$\begin{aligned}
&1 \wedge 1 = 1,\\
&1 \wedge (\underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p}) = \underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p},\\
&(\underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p}) \wedge 1 = \underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p},\\
&(\underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p}) \wedge (\underline{\underline{e}}_{j_1} \wedge \cdots \wedge \underline{\underline{e}}_{j_q}) = \underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p} \wedge \underline{\underline{e}}_{j_1} \cdots \wedge \underline{\underline{e}}_{j_q}.
\end{aligned}$$

Initially, this is given for $i_1 < \cdots < i_p$ and $j_1 < \cdots j_q$, but clearly it remains true in general. We have $\underline{\underline{e}}_i \wedge \underline{\underline{e}}_j = -\underline{\underline{e}}_j \wedge \underline{\underline{e}}_i$. This algebra is associative. Note that this fits in with the original notation $\underline{\underline{e}}_{i_1} \wedge \cdots \wedge \underline{\underline{e}}_{i_p}$. The resulting algebra is called the *Grassman* algebra, or *exterior* algebra. If $\underline{\underline{x}}_1,\dots,\underline{\underline{x}}_p \in K^n$, then

$$\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \in K^n_p.$$

Such a p–vector is called *decomposable.*

LEMMA 5A. *Suppose* $\underline{\underline{x}}_i = (\xi_{i1}, \dots, \xi_{in}) = \sum_{j=1}^n \xi_{ij}\underline{\underline{e}}_j$ $(i = 1, \dots, p)$. *Then*

$$\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p = \sum_{\sigma \in C(n,p)} \xi_\sigma \underline{\underline{E}}_\sigma$$

where ξ_σ *is the* $p \times p$ *determinant* $|\xi_{ij}|$ *with* $1 \leq i \leq p$, $j \in \sigma$.

For example, when $n = 3, p = 2$,

$$\underline{\underline{x}}_1 \wedge \underline{\underline{x}}_2 = \begin{vmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{vmatrix} \underline{\underline{E}}_{12} + \begin{vmatrix} \xi_{11} & \xi_{13} \\ \xi_{21} & \xi_{23} \end{vmatrix} \underline{\underline{E}}_{13} + \begin{vmatrix} \xi_{12} & \xi_{13} \\ \xi_{22} & \xi_{23} \end{vmatrix} \underline{\underline{E}}_{23}.$$

The linear map with $\underline{\underline{E}}_{12} \mapsto \underline{\underline{e}}_3$, $\underline{\underline{E}}_{13} \mapsto -\underline{\underline{e}}_2$, $\underline{\underline{E}}_{23} \mapsto \underline{\underline{e}}_1$ identifies K_2^3 with K^3 and the wedge produced with the cross product.

When $n = 4, p = 2$

$$\underline{\underline{x}}_1 \wedge \underline{\underline{x}}_2 = \begin{vmatrix} \xi_{11} & \xi_{12} \\ \xi_{21} & \xi_{22} \end{vmatrix} \underline{\underline{E}}_{12} + \cdots + \begin{vmatrix} \xi_{13} & \xi_{14} \\ \xi_{23} & \xi_{24} \end{vmatrix} \underline{\underline{E}}_{34},$$

which has six terms.

When $p = n$,

$$\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p = \begin{vmatrix} \xi_{11} & \cdots & \xi_{1n} \\ \vdots & & \\ \xi_{n1} & \cdots & \xi_{nn} \end{vmatrix} \underline{\underline{E}}_{12\cdots n}.$$

Proof. The left-hand side is linear in each vector $\underline{\underline{x}}_i$, the right-hand side is linear, too. So it suffices to consider the case when $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p \in \{\underline{\underline{e}}_1, \dots, \underline{\underline{e}}_n\}$. If two of the $\underline{\underline{x}}_i$'s are the same, then both sides vanish. So without loss of generality $\underline{\underline{x}}_i = \underline{\underline{e}}_{j_i}$, $(i = 1, \dots, p)$ with $j_i \in \{1, \dots, n\}$ distinct. Since both sides behave in obvious ways under permutations of vectors, we may suppose $j_1 < j_2 < \cdots < j_p$. Then the left-hand side is $\underline{\underline{E}}_{j_1 \cdots j_p} = \underline{\underline{E}}_\tau$ where $\tau = \{j_1, \dots, j_p\}$. On the right-hand side $\xi_\sigma = 1$ if $\sigma = \tau$, but $\xi_\sigma = 0$ if $\sigma \neq \tau$, since ξ_σ is the determinant of the submatrix of (ξ_{ij}) with columns $j_1, \dots, j_p$.

A consequence of Lemma 5A is Laplace's expansion of a determinant after a set of rows. For simplicity we will deal only with expansion after the first p rows. Given p, q with $p + q = n$, and given $\sigma \in C(n,p)$, let $\bar{\sigma} \in C(n,q)$ be the complement of σ in $\{1, \dots, n\}$. Let $\varepsilon(\sigma, \bar{\sigma})$ be 1 or -1, depending on whether $(\sigma, \bar{\sigma})$ is an even or an odd permutation of $\{1, \dots, n\}$. Let $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p, \underline{\underline{y}}_1, \dots, \underline{\underline{y}}_q$ be in K^n, and write

$$\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p = \sum_{\sigma \in C(n,p)} \xi_\sigma \underline{\underline{E}}_\sigma, \qquad \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q = \sum_{\tau \in C(n,q)} \eta_\tau \underline{\underline{E}}_\tau.$$

Then

$$\begin{aligned}\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q &= \sum_{\sigma\in C(n,p)} \sum_{\tau\in C(n,q)} \xi_\sigma \eta_\tau \underline{\underline{E}}_\sigma \wedge \underline{\underline{E}}_\tau \\ &= \sum_{\sigma\in C(n,p)} \xi_\sigma \eta_{\bar\sigma} \underline{\underline{E}}_\sigma \wedge \underline{\underline{E}}_{\bar\sigma} \\ &= \sum_{\sigma\in C(n,p)} \varepsilon(\sigma,\bar\sigma) \xi_\sigma \eta_{\bar\sigma} \underline{\underline{E}}_{12\cdots n}.\end{aligned}$$

By Lemma 5A,

$$\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q = (\det M) \underline{\underline{E}}_{12\cdots n}$$

where M is the matrix with rows $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p, \underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_q$. We therefore have

LEMMA 5B. (Laplace expansion of a determinant.)

$$\det M = \sum_{\sigma\in C(n,p)} \varepsilon(\sigma,\bar\sigma)\xi_\sigma\eta_{\bar\sigma}.$$

Note that by Lemma 5A the ξ_σ are the $(p \times p)$–determinants from the rows $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$ of M, and the $\eta_{\bar\sigma}$ are the $(q \times q)$–determinants from the complementary rows $\underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_q$.

LEMMA 5C. *$\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p = \underline{\underline{0}}$ if and only if $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$ are linearly dependent.*

Proof. It is an immediate consequence of Lemma 5A.

LEMMA 5D. *If $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$ are linearly independent and $\underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_p$ are linearly independent, then $\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$ is proportional to $\underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_p$ if and only if $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$ and $\underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_p$ span the same subspace of K^n.*

Proof. If the $\underline{\underline{x}}$'s and $\underline{\underline{y}}$'s span the same subspace, then each $\underline{\underline{y}}_i$ $(i = 1, \ldots, p)$ is a linear combination of $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$, so that $\underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_p$ is a multiple of $\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$. The factor is the determinant of the coefficient matrix for the $\underline{\underline{y}}_i$'s in terms of the $\underline{\underline{x}}_j$'s. Conversely, suppose that $\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p = \lambda(\underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_p)$. For any $\underline{\underline{x}}$, the vector $\underline{\underline{x}} \wedge (\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p) = \underline{\underline{x}} \wedge \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$ is zero precisely when $\underline{\underline{x}}$ lies in the space spanned by $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$. But $\underline{\underline{y}}_i \wedge (\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p) = \lambda(\underline{\underline{y}}_i \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_p) = 0$ since two $\underline{\underline{y}}_i$'s occur. So $\underline{\underline{y}}_i$ is in the space spanned by $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$ $(i = 1, \ldots, p)$. Therefore the spaces are the same.

Let $S^p \subseteq K^n$ be a subspace of dimension p. Let $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$ be a basis of S^p. Then let $\underline{\underline{X}} = \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$, which is a vector with $\ell = \binom{n}{p}$ components and which lies in $K^n_p \approx K^\ell$. The components of $\underline{\underline{X}}$ are called the "*Grassman coordinates* of S_p". By the lemma, the Grassman coordinates are given up to a factor. Grassman coordinates of distinct p–dimensional subspaces are not proportional. Incidentally, the Grassman coordinates in general do not fill all of K_p^n, i.e., not every p–vector is decomposable. A heuristic argument is that the p–dimensional subspaces of K^n constitute a "manifold" with $p(n-p)$ degrees of freedom, so that the Grassman coordinates should be a manifold of dimension $p(n-p)+1$, and for most cases with $0 < p < n$ we have $p(n-p)+1 < \binom{n}{p} = \dim K_p^n$.

Now suppose that $K = \mathbb{R}$ or $\mathbb{C}$. Make $\mathbb{R}^n$ into a Euclidean space or introduce a Hermitian metric on $\mathbb{C}^n$ with $\underline{\underline{e}}_i\underline{\underline{e}}_j = \delta_{ij}$ $(i \leqq i,\ j \leqq n)$. Thus in the Hermitian case, if $\underline{\underline{x}} = (\xi_1, \dots, \xi_n)$, $\underline{\underline{y}} = (\eta_1, \dots, \eta_n)$, then $\underline{\underline{x}}\overline{\underline{\underline{y}}} = \xi_1\bar{\eta}_1 + \cdots + \xi_n\bar{\eta}_n$. Introduce a similar metric on K_p^n with

$$\underline{\underline{E}}_\sigma \underline{\underline{E}}_\tau = \left\{ \begin{array}{ll} 1 & \text{if } \sigma = \tau, \\ 0 & \text{otherwise.} \end{array} \right\} = \delta_{\sigma\tau},$$

say.

LEMMA 5E. (Laplace identity.) *Given* $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p, \underline{\underline{y}}_1, \dots, \underline{\underline{y}}_p$ *in* $\mathbb{R}^n$ *(or* $\mathbb{C}^n$*), we have*

$$(\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p) \cdot (\underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_p) = \begin{vmatrix} \underline{\underline{x}}_1 \underline{\underline{y}}_1 & \cdots & \underline{\underline{x}}_1 \underline{\underline{y}}_p \\ \vdots & & \vdots \\ \underline{\underline{x}}_p \underline{\underline{y}}_1 & \cdots & \underline{\underline{x}}_p \underline{\underline{y}}_p \end{vmatrix}.$$

Here the inner product of the left-hand side is in $\mathbb{R}_p^n$ (or $\mathbb{C}_p^n$), but each inner product on the right-hand side is in $\mathbb{R}^n$ (or $\mathbb{C}^n$).

Exercise 5a. Prove Lemma 5E, using linearity.

A consequence of the Laplace identity is that

$$|\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p| = \begin{vmatrix} \underline{\underline{x}}_1 \underline{\underline{y}}_1 & \cdots & \underline{\underline{x}}_1 \underline{\underline{x}}_p \\ \vdots & & \vdots \\ \underline{\underline{x}}_p \underline{\underline{x}}_1 & \cdots & \underline{\underline{x}}_p \underline{\underline{x}}_p \end{vmatrix}^{1/2}.$$

As we have seen, this is the volume of the p–dimensional parallelepiped spanned by $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p$.

LEMMA 5F. *For any* $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p, \underline{\underline{y}}_1, \dots, \underline{\underline{y}}_q$,

(i) $|\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q| \leqq |\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p||\underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|$, *where equality holds* *** *if* $\underline{\underline{x}}_i \underline{\underline{y}}_j = 0$ $(1 \leqq i \leqq p,\ 1 \leqq j \leqq q)$.

(ii) *For any* $\underline{\underline{u}}_1, \dots, \underline{\underline{u}}_\ell, \underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p$, *and* $\underline{\underline{y}}_1 \dots, \underline{\underline{y}}_q$,

$$|\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell| \cdot |\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell \wedge \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|$$
$$\leqq |\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell \wedge \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p||\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|.$$

***There are other cases of equality, e.g. when $\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p = \underline{\underline{0}}$ or $\underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q = \underline{\underline{0}}$.

There is a geometric interpretation to (i): The volume of the $(p+q)$–dimensional parallelepiped spanned by $\underline{\underline{x}}_1,\dots,\underline{\underline{x}}_p, \underline{\underline{y}}_1,\dots,\underline{\underline{y}}_q$ does not exceed the product of the volumes of the p–dimensional parallelepiped spanned by $\underline{\underline{x}}_1,\dots,\underline{\underline{x}}_p$ and the q–dimensional parallelepiped spanned by $\underline{\underline{y}}_1,\dots,\underline{\underline{y}}_q$. This is well-known, e.g. when $p=2$, $q=1$.

Proof. The length of a wedge product is invariant under orthogonal (unitary) linear transformations in $\mathbb{R}^n$ (or $\mathbb{C}^n$)

(i) is obvious if $\underline{\underline{x}}_1,\dots,\underline{\underline{x}}_p, \underline{\underline{y}}_1,\dots\underline{\underline{y}}_q$ are linearly dependent. So we may assume that $\underline{\underline{x}}_1,\dots,\underline{\underline{x}}_p, \underline{\underline{y}}_1,\dots,\underline{\underline{y}}_q$ span a space S of dimension $m=p+q$. After a suitable orthogonal (or unitary) transformation, S consists of points $(\xi_1,\dots,\xi_m,0,\dots,0)$. So we may write $\underline{\underline{x}}_i=(\xi_{i1},\dots,\xi_{im},0,\dots,0)$ and $\underline{\underline{y}}_j=(\eta_{j1},\dots,\eta_{jm},0,\dots,0)$ $(i=1,\dots,p;\ j=1,\dots,q)$. Then

$$\underline{\underline{x}}_1\wedge\cdots\wedge\underline{\underline{x}}_p\wedge\underline{\underline{y}}_1\wedge\cdots\wedge\underline{\underline{y}}_q=\left(\begin{vmatrix}\xi_{11}&\cdots&\xi_{1p}&\cdots&\xi_{1m}\\ \vdots&&\vdots&&\vdots\\ \xi_{p1}&\cdots&\xi_{pp}&\cdots&\xi_{pm}\\ \eta_{11}&\cdots&\eta_{1p}&\cdots&\eta_{1m}\\ \vdots&&&&\\ \eta_{q1}&\cdots&\eta_{qp}&\cdots&\eta_{qm}\end{vmatrix},0,\dots,0\right).$$

The length is the absolute value of this $m\times m$ determinant. $\underline{\underline{x}}_1\wedge\cdots\wedge\underline{\underline{x}}_p$ has coordinates which are the $p\times p$ determinants from (ξ_{ij}) and $\underline{\underline{y}}_1\wedge\cdots\wedge\underline{\underline{y}}_q$ has coordinates which are the $(q\times q)$ determinants from (η_{ij}). The first assertion of (i) follows from Laplace's expansion of the $m\times m$ determinant with respect to the first p rows and last q rows and from Cauchy's inequality. (Laplace's expansion has $\binom{m}{p}=\binom{m}{q}$ summands.)

For (ii), we can write $\underline{\underline{x}}_i=\underline{\underline{x}}'_i+\underline{\underline{x}}''_i$ $(i=1,\dots,p)$ where the $\underline{\underline{x}}''_i$'s are spanned by the $\underline{\underline{u}}$'s and the $\underline{\underline{x}}'_i$'s are orthogonal to the $\underline{\underline{u}}$'s $(i=1,\dots,p)$. Similarly, $\underline{\underline{y}}_j=\underline{\underline{y}}'_j+\underline{\underline{y}}''_j$ $(j=1,\dots,q)$. The exterior products in (ii) are unchanged if we replace $\underline{\underline{x}}_i$'s with $\underline{\underline{x}}'_i$'s and $\underline{\underline{y}}_i$'s with $\underline{\underline{y}}'_i$'s. So we may suppose, without loss of generality, that $\underline{\underline{x}}_i\underline{\underline{u}}_s=0$, $\underline{\underline{y}}_j\underline{\underline{u}}_s=0$ $(i=1,\dots,p;\ j=1,\dots,q;\ s=1,\dots,\ell)$. Then, using the second assertion in (i), the left-hand side becomes

$$|\underline{\underline{u}}_1\wedge\cdots\wedge\underline{\underline{u}}_\ell|^2|\underline{\underline{x}}_1\wedge\cdots\wedge\underline{\underline{x}}_p\wedge\underline{\underline{y}}_1\wedge\cdots\wedge\underline{\underline{y}}_q|,$$

the right-hand side becomes

$$|\underline{\underline{u}}_1\wedge\cdots\wedge\underline{\underline{u}}_\ell|^2|\underline{\underline{x}}_1\wedge\cdots\wedge\underline{\underline{x}}_p||\underline{\underline{y}}_1\wedge\cdots\wedge\underline{\underline{y}}_q|,$$

and (ii) follows.

Let p,q be positive integers with $p+q=n$. Let K^n be $\mathbb{R}^n$ or $\mathbb{C}^n$, equipped with the usual Euclidean or Hermitian metric. Let S^p, T^q be subspaces of respective dimensions p,q which are orthogonal complements of each other.

LEMMA 5G. *If $\{\xi_\sigma\}$ is a Grassman coordinate vector for S^p, then $\{\eta_\tau\}$ with*

$$\eta_\tau = \varepsilon(\bar{\tau}, \tau)\bar{\xi}_{\bar{\tau}}$$

is a Grassman coordinate vector for T^q. (Here $\bar{\tau}$ denotes the complement but $\bar{\xi}$ the complex conjugate).

Example. Let $p = 2$, $q = 1$. Suppose S^2 is spanned by (x_{11}, x_{12}, x_{13}) and (x_{21}, x_{22}, x_{23}). A set of Grassman coordinates will be $(\xi_{12}, \xi_{13}, \xi_{23}) = \left(\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}, \begin{vmatrix} x_{11} & x_{13} \\ x_{21} & x_{23} \end{vmatrix}, \begin{vmatrix} x_{12} & x_{13} \\ x_{22} & x_{23} \end{vmatrix}\right)$. But T^1 is spanned by $(\xi_{23}, -\xi_{13}, \xi_{23})$, so that its Grassman coordinates are $(\xi_{23}, -\xi_{13}, \xi_{12})$. So the lemma holds.

Proof.‡ Let $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p$ be a basis for S^p and $\underline{\underline{y}}_1, \dots, \underline{\underline{y}}_q$ a basis for T^q. Write $\underline{\underline{X}} = \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$, $\underline{\underline{Y}} = \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q$. Discarding the notation in the statement of the Lemma, write

$$\underline{\underline{X}} = \sum_{\sigma \in C(n,p)} \xi_\sigma \underline{\underline{E}}_\sigma, \qquad \underline{\underline{Y}} = \sum_{\tau \in C(n,p)} \eta_\tau \underline{\underline{E}}_\tau.$$

By Lemma 5F we have $|\underline{\underline{X}} \wedge \underline{\underline{Y}}| = |\underline{\underline{Y}}||\underline{\underline{Y}}|$. We obtain

$$\begin{aligned}
|\underline{\underline{X}}|^2 |\underline{\underline{Y}}|^2 &= |\underline{\underline{X}} \wedge \underline{\underline{Y}}|^2 \\
&= \left| \sum_\sigma \sum_\tau \xi_\sigma \eta_\tau \underline{\underline{E}}_\sigma \wedge \underline{\underline{E}}_\tau \right|^2 \\
&= \left| \sum_\sigma \xi_\sigma \eta_{\bar{\sigma}} \varepsilon(\sigma, \bar{\sigma}) \underline{\underline{E}}_{12\cdots n} \right|^2 \\
&= \left| \sum_{\tau \in C(n,q)} (\varepsilon(\bar{\tau}, \tau)\xi_{\bar{\tau}})\eta_\tau \right|^2 \\
&\leqq \left(\sum_{\tau \in C(n,q)} |\xi_{\bar{\tau}}|^2 \right) \left(\sum_{\tau \in C(n,q)} |\eta_\tau|^2 \right) \\
&= |\underline{\underline{X}}|^2 |\underline{\underline{Y}}|^2.
\end{aligned}$$

Hence, since the Cauchy–Schwartz inequality is an equality, the vector $\{\eta_\tau\}$ must be a multiple of the vector $\{\varepsilon(\bar{\tau}, \tau)\bar{\xi}_{\bar{\tau}}\}$. The Lemma follows.

Suppose S^p is a rational subspace of $\mathbb{R}^n$ and $\Lambda = \Lambda(S^p)$ is the lattice of integer points in S^p. Let $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p$ be a basis for Λ. Then

$$\underline{\underline{X}} = \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$$

‡This proof was suggested by Prof. L. Baggett.

will be a set of Grassman coordinates for S^k.

LEMMA 5H. *The components of $\underline{\underline{X}}$ are relatively prime.*

Proof. Suppose the components of $\underline{\underline{X}}$ have a common prime factor ℓ. Then the matrix

$$\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \\ x_{p1} & \cdots & x_{pn} \end{pmatrix}$$

modulo ℓ is singular. So there exist integers $c_1, \ldots, c_p$, not all congruent to 0 mod ℓ, such that $c_1\underline{\underline{x}}_1 + \cdots + c_p\underline{\underline{x}}_p \equiv 0 \pmod{\ell}$. Without loss of generality, $c_1 \not\equiv 0 \pmod{\ell}$. Then take $\underline{\underline{x}}_1' = \frac{1}{\ell}(c_1\underline{\underline{x}}_1 + \cdots + c_p\underline{\underline{x}}_p) \in \Lambda$. But $\underline{\underline{x}}_1'$ is not a linear combination with integer coefficients of $\underline{\underline{x}}_1, \ldots, \underline{\underline{x}}_p$. Contradiction, since the $\underline{\underline{x}}_i$'s form a basis.

COROLLARY 5I. $H(S^p) = |\underline{\underline{X}}|$, *where $\underline{\underline{X}}$ is a Grassman coordinate vector with coprime components of the rational subspace S^p.*

COROLLARY 5J. *When S is a rational subspace, its orthogonal complement $S^\perp$ has*

$$H(S^\perp) = H(S).$$

Proof. Let $\underline{\underline{X}}$ be a Grassman coordinate vector of S with coprime integer components. By Lemma 5G, $S^\perp$ has a Grassman coordinate vector whose components are the same as those of $\underline{\underline{X}}$, except for signs and ordering.

§6. Absolute Values.

An absolute value is a map $a \longmapsto |a|$ from a field K to the reals such that

$$\begin{aligned} &|a| \geqq 0, \quad \text{and} \quad |a| = 0 \quad \text{precisely when} \quad a = 0, \\ &|ab| = |a||b|, \\ &|a+b| \leqq |a| + |b|. \end{aligned}$$

The last relation is called *triangle inequality*. When $K = \mathbb{Q}$, the standard absolute value is an absolute value in our sense. In order to avoid confusion with other possible absolute values, we will denote it by $|a|_\infty$. For any prime p, we can write any nonzero $a \in \mathbb{Q}$ as $a = p^\alpha(u/v)$ where $p \mid uv$. The p–adic absolute value is defined by

$$|a|_p = \begin{cases} p^{-\alpha} & \text{if} \quad a \neq 0, \\ 0 \quad \text{if} & a = 0. \end{cases}$$

Then $|a|_p$ satisfies all the axioms of an absolute value. In fact we have $|a+b|_p \leqq \max(|a|_p, |b|_p)$, which is stronger than the triangle inequality. An absolute value with

$$|a+b| \leqq \max(|a|, |b|) \tag{6.1}$$

is called *non-Archimedean.* Absolute values which don't satisfy (6.1) are called *Archimedean.*

Let $M(\mathbb{Q}) = \{\infty, 2, 3, 5, \dots\}$. For $v \in M(\mathbb{Q})$, the absolute value $|\ |_v$ is Archimedean precisely when $v = \infty$. If $a \in \mathbb{Q}$ is nonzero, we have the product formula

$$\prod_{v \in M(\mathbb{Q})} |a|_v = 1.$$

LEMMA 6A. *Let $|\dots|$ be an absolute value on a field K of characteristic zero. This absolute value is non-Archimedean if and only if $|n| \leqq 1$ for every $n \in \mathbb{Z}$.*

Proof. $|1| = |1||1|$, so that $|1| = 1$. Also $|1| = |-1||-1|$, so that $|-1| = 1$. In the case of a non-Archimedean absolute value one now proves easily by induction on $n > 0$ that $|n| \leqq 1$, and therefore also $|-n| = |n| \leqq 1$.

Conversely, suppose that $|n| \leqq 1$ for $n \in \mathbb{Z}$. We have

$$(a+b)^\nu = \sum_{i=0}^{\nu} \binom{\nu}{i} a^i b^{\nu-i},$$

therefore

$$|a+b|^\nu \leqq \sum_{i=0}^{\nu} \left|\binom{\nu}{i}\right| |a|^i |b|^{\nu-i} \leqq \sum_{i=0}^{\nu} |a|^i |b|^{\nu-i} \leqq (\nu+1) N^\nu$$

where $N = \max(|a|, |b|)$. Taking ν-th roots we get

$$|a+b| \leqq \sqrt[\nu]{\nu+1}\, N,$$

and letting $\nu \to \infty$ we obtain $|a+b| \leqq N = \max(|a|, |b|)$.

The absolute value with $|a| = 1$ for every $a \neq 0$ in K is called *trivial.*

THEOREM 6B. (Ostrowski (1935)) *The non-trivial absolute values on $\mathbb{Q}$ are given by*

$$|a| = |a|_\infty^\rho \quad \textit{where} \quad 0 < \rho \leqq 1$$

and

$$|a| = |a|_p^\sigma \quad \textit{where} \quad \sigma > 0.$$

Proof. One proves by induction on positive integers $n > 0$ that $|n| \leqq n$, so that also $|-n| \leqq n$, and

$$|n| \leqq |n|_\infty.$$

Let $a, b \in \mathbb{Z}$ with $a > 1$, $b > 1$. For $\nu > 0$, we can write $b^\nu = c_0 + c_1 a + \cdots + c_n a^n$ with $0 \leqq c_i < a$ and $c_n \neq 0$. Then

$$\begin{aligned} |b|^\nu = |b^\nu| &\leqq |c_0| + |c_1||a| + \cdots + |c_n||a|^n \\ &\leqq (n+1) a M^n \\ &\leqq \left(1 + \frac{\nu \log b}{\log a}\right) a M^n, \end{aligned}$$

where $M = \max(1, |a|)$. Taking ν-th roots gives

$$|b| \leqq \sqrt[\nu]{1 + \frac{\nu \log b}{\log a}}\ \sqrt[\nu]{a}\, M^{\log b / \log a}.$$

And letting $\nu \to \infty$ gives

$$|b| \leqq M^{\log b / \log a}.$$

That is,

$$|b| \leqq \max(1, |a|^{\log b / \log a}). \tag{6.2}$$

Case I. $|\ |$ Archimedean. By Lemma 6A, there exists an integer b with $|b| > 1$. Then by (6.2) $|a| > 1$ for any $a \in \mathbb{Z}$ with $a > 1$. So $|a| > 1$ for any $a \in \mathbb{Z}$ with $a \notin \{-1, 0, -1\}$. For $a, b \in \mathbb{Z}$ and $a, b > 1$, we have from the above that

$$\begin{aligned} |b| &\leqq \max(1, |a|^{\log b / \log a}) \\ &= |a|^{\log b / \log a}. \end{aligned}$$

Then

$$|b|^{1/\log b} \leqq |a|^{1/\log a}.$$

By symmetry, we get equality, i.e.

$$|b|^{1/\log b} = |a|^{1/\log a}. \tag{6.3}$$

We have $1 < |b| \leqq |b|_\infty = b$. So $|b| = b^\rho$ with $0 < \rho \leqq 1$ and then $|a| = a^\rho = |a|_\infty^\rho$ by (6.3). Then for any rational r, we get $|r| = |r|_\infty^\rho$.

Case II. $|\ |$ non-Archimedean. We have $|n| \leqq 1$ for every $n \in \mathbb{Z}$. Since $|\ |$ is non-trivial, there exists $a \in \mathbb{Z}$ with $|a| < 1$. Let $I = \{a \in \mathbb{Z} : |a| < 1\}$. Then I is an ideal in $\mathbb{Z}$. If $|ab| < 1$, then $|a| < 1$ or $|b| < 1$ since $|ab| = |a||b|$. So I is a prime ideal, say $I = (p)$.

Now let $r \in \mathbb{Q}$ with $r \neq 0$. Write $r = p^\nu x / y$ with $x, y \in \mathbb{Z}$ and $p \mid xy$. Then $x, y \notin I$ so $|x| = |y| = 1$ and

$$|r| = |p^\nu| = |p|^\nu.$$

Since $p \in I$, we have $|p| < 1$ so

$$|p| = p^{-\sigma} \quad \text{with} \quad \sigma > 0.$$

Then

$$|r| = |p|^{\nu} = p^{-\sigma\nu} = (p^{-\nu})^{\sigma} = |r|_p^{\sigma}$$

with $\sigma > 0$.

We now turn to algebraic number fields. With each algebraic number field K there is associated a set $M(K)$ along with certain absolute values $|a|_v$ where $v \in M(K)$. We have $| \ |_v \neq | \ |_{v'}$ if $v \neq v'$ and the following:

(i) $M(\mathbb{Q}) = \{\infty, 2, 3, 5, \dots\}$.

(ii) For any $a \in K$, $a \neq 0$, we have $|a|_v = 1$ for all but finitely many $v \in M(K)$.

(iii) With every v is associated a natural number n_v such that for $a \neq 0$ in K we have the product formula

$$\prod_{v \in M(K)} |a|_v^{n_v} = 1.$$

For $v \in M(\mathbb{Q})$, $n_v = 1$.

(iv) If $K' \subset K$ and $v \in M(K)$, then there is a $v' \in M(K)$ such that $|a|_v$ restricted to $a \in K'$ equals $|a|_{v'}$. This v' is unique and $n_{v'} \mid n_v$. We write $v \mid v'$.

(v) If $K' \subset K$ and $v' \in M(K')$, then there are finitely many $v \in M(K)$ with $v \mid v'$ and

$$\sum_{\substack{v \in M(K) \\ v \mid v'}} \frac{n_v}{n_{v'}} = [K : K'].$$

In particular, by (iii), (v), given $v' \in M(\mathbb{Q})$ we have

$$\sum_{\substack{v \in M(K) \\ v \mid v'}} n_v = [K : \mathbb{Q}]$$

(vi) If K is an algebraic extension of $\mathbb{Q}$ with r_1 real embeddings mapping $a \in K$ respectively into $a^{(1)}, \dots, a^{(r_1)}$ and r_2 pairs of complex conjugate embeddings mapping a into

$$a^{(r_1+1)}, \overline{a^{(r_1+1)}}, \dots, a^{(r_1+r_2)}, \overline{a^{(r_1+r_2)}}$$

where $r_1 + 2r_2 = [K : \mathbb{Q}]$, then the absolute values dividing ∞ are

$$|a^{(1)}|, \dots, |a^{(r_1)}|, |a^{(r_1+1)}|, \dots, |a^{(r_1+r_2)}|.$$

The first r_1 of these have $n_v = 1$ and the last r_2 have $n_v = 2$.

(vii) Let $\sigma : K \to L$ be an isomorphism. If $v \in M(L)$, for $a \in K$ put $|a|_w = |\sigma a|_v$. Then $w \in M(K)$, and this gives a one–to–one map $M(L) \to M(K)$, and in this correspondence $n_v = n_w$.

We listed these properties in an axiomatic way but don't intend to prove them. They can be found in any treatment of algebraic number fields based on absolute values. For readers more familiar with classical ideal theory we now sketch the connection with ideals.

With any algebraic number field K there is associated a ring $\mathfrak{O}$ of integers in K. Any nonzero ideal $\mathfrak{A} \subseteq \mathfrak{O}$ can uniquely be written as a product of prime ideals, i.e., $\mathfrak{A} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_\ell^{a_\ell}$ with nonnegative integers $a_1, \dots, a_\ell$. In particular, any principal ideal (p) can be factored in this manner, $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_\ell^{e_\ell}$, where $\mathfrak{P}_i \mid p$. We can define norms of these prime ideals by $\mathfrak{N}(\mathfrak{P}_i) = p^{f_i}$ where $\mathrm{card}(\mathfrak{O}/\mathfrak{P}_i) = p^{f_i}$. A fractional nonzero ideal $\mathfrak{A}$ can also uniquely be written as $\mathfrak{A} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_\ell^{a_\ell}$ with $a_1, \dots, a_\ell$ in $\mathbb{Z}$.

Non-Archimedean absolute values $|\ |_v$ with $v \in M(K)$ are in one–to–one correspondence with prime ideals. That is, $|a|_{\mathfrak{P}} = p^{-\nu/e}$ if $(a) = \mathfrak{P}^\nu \mathfrak{A}$ where $\mathfrak{P} \mid p$ and $(p) = \mathfrak{P}^e \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_\ell^{e_\ell}$, and where $\mathfrak{P}$ does not occur in the factorization of $\mathfrak{A}$. So $|p|_{\mathfrak{P}} = p^{-1} = |p|_p$ and $|\ |_{\mathfrak{P}}$ extends $|\ |_p$. We also have $n_{\mathfrak{P}} = ef$ where $\mathfrak{N}(\mathfrak{P}) = p^f$.

Example: Let $K = \mathbb{Q}(\sqrt{2})$. Then $7 = (3+\sqrt{2})(3-\sqrt{2})$ in K. By (vi), there are two absolute values dividing ∞. Say $v_1 \mid \infty$ and $v_2 \mid \infty$. Then $n_{v_1} = n_{v_2} = 1$. And we have $|3+\sqrt{2}|_{v_1} = 3+\sqrt{2}$, $|3-\sqrt{2}|_{v_1} = 3-\sqrt{2}$, $|3+\sqrt{2}|_{v_2} = 3-\sqrt{2}$, $|3-\sqrt{2}|_{v_2} = 3+\sqrt{2}$. Now look at the absolute values dividing 7. $\mathfrak{P}_1 = (3+\sqrt{2})$, $\mathfrak{P}_2 = (3-\sqrt{2})$ divide 7. If w_1, w_2 are the absolute values associated with $\mathfrak{P}_1, \mathfrak{P}_2$ we have $n_{w_1} = n_{w_2} = 1$ and $|3+\sqrt{2}|_{w_1} = 7^{-1}$, $|3-\sqrt{2}|_{w_1} = 1$, $|3+\sqrt{2}|_{w_2} = 1$, $|3-\sqrt{2}|_{w_2} = 7^{-1}$. For $u \neq v_1, v_2, w_1, w_2$, $|3+\sqrt{2}|_u = 1$, so the product formula holds for $a = 3+\sqrt{2}$ and $a = 3-\sqrt{2}$.

Remark. If $v \mid \infty$, then $|\ |_v$ is Archimedean. If $v \mid \infty$, then $|\ |_v$ is non-Archimedean. This follows from Lemma 6A.

§7. Heights in Number Fields.

Consider $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in K^n$. Define

$$|\underline{\alpha}|_v = \begin{cases} (|\alpha_1|_v^2 + \cdots + |\alpha_n|_v^2)^{1/2} & \text{if } \ v \text{ is Archimedean} \\ \max(|\alpha_1|_v, \dots, |\alpha_n|_v) & \text{if } \ v \text{ is non-Archimedean.} \end{cases}$$

If $\underline{\alpha} \neq \underline{0}$, then $|\underline{\alpha}|_v = 1$ for all but finitely many v. For $\underline{\alpha} \neq \underline{0}$, define the *height* (or "field height") of $\underline{\alpha}$ by

$$H_K(\underline{\alpha}) = \prod_{v \in M(K)} |\underline{\alpha}|_v^{n_v}.$$

If, e.g., $\alpha_1 \neq 0$, then $|\underline{\alpha}|_v \geqq |\alpha_1|_v$ for each v, which implies $H_K(\underline{\alpha}) \geqq 1$. Also $|\lambda\underline{\alpha}|_v = |\lambda|_v |\underline{\alpha}|_v$, so $H_K(\lambda\underline{\alpha}) = H_K(\underline{\alpha})$ for $\lambda \neq 0$ by the product formula.

Example. Take $K = \mathbb{Q}$. Let $\underline{x} = (x_1, \dots, x_n)$ be a primitive integer point. We have $|\underline{x}|_\infty = |\underline{x}|$ (the usual Euclidean norm) and $|\underline{x}|_p = \max(|x_1|_p, \dots, |x_n|_p) = 1$ for every $p \neq \infty$, since $\underline{x}$ is primitive. So $H_{\mathbb{Q}}(\underline{x}) = |\underline{x}|$.

Example. Take $K = \mathbb{Q}(\sqrt{2})$. Let $\underline{\alpha} = (1, 3+\sqrt{2})$. We have $|\underline{\alpha}|_{v_1} = \sqrt{1^2 + (3+\sqrt{2})^2}$ $= \sqrt{6}\sqrt{2+\sqrt{2}}$, $|\underline{\alpha}|_{v_2} = \sqrt{6}\sqrt{2-\sqrt{2}}$, $|\underline{\alpha}|_{w_1} = |\underline{\alpha}|_{w_2} = 1$, in fact $|\underline{\alpha}|_u = 1$ for u non-Archimedean in $M(K)$. So $H_K(\underline{\alpha}) = |\underline{\alpha}|_{v_1} |\underline{\alpha}|_{v_2} = 6\sqrt{2}$.

Suppose $K \subset \hat{K}$ and $\underline{\underline{\alpha}} \in K^n$, $\underline{\underline{\alpha}} \neq 0$. Then how do $H_K(\underline{\underline{\alpha}})$ and $H_{\hat{K}}(\underline{\underline{\alpha}})$ compare?

$$H_{\hat{K}}(\underline{\underline{\alpha}}) = \prod_{\hat{v} \in M(\hat{K})} |\underline{\underline{\alpha}}|_{\hat{v}}^{n_{\hat{v}}} = \prod_{v \in M(K)} \prod_{\substack{\hat{v} \in M(\hat{K}) \\ \hat{v}|v}} |\alpha|_v^{n_{\hat{v}}}.$$

And (v) of section 6 gives

$$\begin{aligned} H_{\hat{K}}(\underline{\underline{\alpha}}) &= \prod_{v \in M(K)} |\underline{\underline{\alpha}}|_v^{n_v[\hat{K}:K]} \\ &= (H_K(\underline{\underline{\alpha}}))^{[\hat{K}:K]}. \end{aligned}$$

The *absolute height* $H(\underline{\underline{\alpha}})$ is defined by

$$H(\underline{\underline{\alpha}}) = H_K(\underline{\underline{\alpha}})^{1/[K:\mathbb{Q}]}.$$

Then $H(\underline{\underline{\alpha}})$ does not depend on the field K.

Remark. If $K \cong L$ and $\sigma : K \to L$ an isomorphism, $\underline{\underline{\alpha}} \in K^n$, $\sigma\underline{\underline{\alpha}} \in L^n$, then by (vii) $H_K(\underline{\underline{\alpha}}) = H_L(\sigma\underline{\underline{\alpha}})$ and $H(\underline{\underline{\alpha}}) = H(\sigma\underline{\underline{\alpha}})$. So conjugate vectors have the same height.

Exercise 7a. Is it possible to estimate $H(\underline{\underline{\alpha}} + \underline{\underline{\beta}})$ in terms of $H(\underline{\underline{\alpha}})$ and $H(\underline{\underline{\beta}})$? You would need to supppose $\underline{\underline{\alpha}} \neq \underline{\underline{0}}$, $\underline{\underline{\beta}} \neq \underline{\underline{0}}$, $\underline{\underline{\alpha}} + \underline{\underline{\beta}} \neq \underline{\underline{0}}$.

If $P(X) = \alpha_n X^n + \cdots + \alpha_1 X + \alpha_0$ with $\alpha_i \in K$ is a nonzero polynomial, define the *height* by

$$H_K(P) = H_K(\alpha_n, \ldots, \alpha_1, \alpha_0).$$

We can define $H(P)$, the *absolute height of a polynomial*, in a similar fashion.

LEMMA 7A.

$$H(PQ) \leq \sqrt{n+1}\, H(P)H(Q)$$

when $\deg P = n$, (*or* $n = \min(\deg P, \deg Q)$).

Proof. Write $P = \alpha_n X^n + \cdots + \alpha_0$. Associate P with $\underline{\underline{\alpha}} = (\alpha_n, \ldots, \alpha_0)$. Define $|P|_v = |\underline{\underline{\alpha}}|_v$. Then

$$H_K(P) = \prod_{v \in M(K)} |P|_v^{n_v}.$$

Suppose v is non-Archimedean. Then

$$|PQ|_v = |P|_v |Q|_v.$$

This is essentially Gauss' Lemma. We leave its proof as **Exercise 7b.** Now write $Q = \beta_m X^m + \cdots + \beta_0$ and $PQ = \gamma_{n+m} X^{n+m} + \cdots + \gamma_0$, where $\gamma_i = \sum_{a+b=i} \alpha_a \beta_b$. If v is Archimedean, then

$$|PQ|_v^2 = \sum_i |\gamma_i|_v^2 = \sum_i \left| \sum_{a+b=i} \alpha_a \beta_b \right|^2.$$

Cauchy's inequality implies that

$$\left|\sum_{k=1}^{N} \delta_k\right|^2 \leqq N \sum_{k=1}^{N} |\delta_k|^2.$$

Using this inequality we obtain

$$\begin{aligned}|PQ|_v^2 &\leqq \sum_{i=0}^{n+m} (n+1) \sum_{\substack{a+b=i \\ 0 \leqq a \leqq n}} |\alpha_a \beta_b|^2 \\ &= (n+1) \sum_a |a_\alpha|^2 \sum_b |\beta_b|^2 \\ &= (n+1) |P|_v^2 |Q|_v^2.\end{aligned}$$

So

$$|PQ|_v \leqq \sqrt{n+1}\, |P|_v |Q|_v$$

if v is Archimedean. Then

$$H_K(PQ) \leqq (n+1)^{\frac{1}{2}\cdot[K:\mathbb{Q}]} H_K(P) H_K(Q)$$

since $\sum_{v|\infty} n_v = [K:\mathbb{Q}]$. And

$$H(PQ) \leqq (n+1)^{1/2} H(P) H(Q).$$

For $\alpha \in K^1 = K$ we have $H_K(\alpha) = H_K(1) = 1$. This doesn't tell us much about α, so we define

$$h_K(\alpha) = H_K(1, \alpha)$$

and

$$h(\alpha) = H(1, \alpha).$$

Then

$$\begin{aligned}h_K(\alpha) &= \prod_{v \in M(K)} |(1, \alpha)|_v^{n_v} \\ &= \left(\prod_{\substack{v \in M(K) \\ v \text{ Archimedean}}} (\sqrt{1 + |\alpha|_v^2}\,)^{n_v} \right) \left(\prod_{\substack{v \in M(K) \\ v \text{ non-Archimedean}}} (\max(1, |\alpha|_v))^{n_v} \right).\end{aligned}$$

Remark. We have $h(1/\alpha) = H(1, 1/\alpha) = H(\alpha, 1) = h(\alpha)$.

Remark. The reader should be warned that other authors often use another height, with the maximum norm for both Archimedean and non-Archimedean absolute values. This is true, e.g., of Bombieri and Van der Poorten (1987) or Mueller and Schmidt (1989). But Bombieri and Vaaler (1983) use the same norm as in these Notes.

Example. Let $a/b \in \mathbb{Q}$ be in lowest terms. Then $h_{\mathbb{Q}}(a/b) = H_{\mathbb{Q}}(1, a/b) = H_{\mathbb{Q}}(b, a) = \sqrt{a^2 + b^2}$.

Exercise 7c. Estimate $h(\alpha\beta)$ and $h(\alpha + \beta)$ in terms of $h(\alpha), h(\beta)$.

LEMMA 7B. *If* $P(X) = \alpha_d(X - \gamma_1) \cdots (X - \gamma_d)$ *where* $\alpha_d, \gamma_1, \ldots, \gamma_d$ *are algebraic, then*

$$5^{-d/2} h(\gamma_1) \cdots h(\gamma_d) \leqq H(P) \leqq 2^{(d-1)/2} h(\gamma_1) \cdots h(\gamma_d).$$

Remark. Notice that the leading coefficient α_d doesn't enter into the inequalities since the height of a polynomial is independent of multiplication by a constant factor.

Proof. The upper limit follows on applying Lemma 7A, $d-1$ times. That gives

$$H(P) \leqq 2^{(d-1)/2} H(X - \gamma_1) \cdots H(X - \gamma_d).$$

Notice that $H(X - \gamma) = H(1, -\gamma) = H(1, \gamma) = h(\gamma)$, so the upper bound is proven.

For the lower bound, we may suppose that $\alpha_d = 1$. If v is non-Archimedean, then

$$\prod_{i=1}^{d} \max(1, |\gamma_i|_v) = |P|_v$$

by Gauss' Lemma. If v is Archimedean, then we claim that

$$\prod_{i=1}^{d} \sqrt{1 + |\gamma_i|_v^2} < 5^{d/2} |P|_v.$$

(This claim will be proven below.) If K is a number field of degree n containing all of the γ's, then

$$\prod_{i=1}^{d} h_K(\gamma_i) < 5^{nd/2} H_K(P).$$

Taking n-th roots gives the result

$$\prod_{i=1}^{d} h(\gamma_i) < 5^{d/2} H(P).$$

The proof‡ of the claim is by induction on d. The case $d = 1$ is trivial. For v Archimedean, we may think of $|\ |_v$ as the usual absolute value on $\mathbb{C}$. Without loss of generality, we have $|\gamma_1| \leqq \cdots \leqq |\gamma_d|$, and we may suppose that $|\gamma_d| \geqq 2$. (Otherwise the result is clear.) Write

$$\begin{aligned} P(X) &= X^d + \alpha_{d-1} X^{d-1} + \cdots + \alpha_0 \\ &= Q(X)(X - \gamma_d) \end{aligned}$$

‡I am indebted to Prof. Halberstam for simplifying my original proof.

where $Q(X) = X^{d-1} + \beta_{d-2}X^{d-2} + \cdots + \beta_0$. Then

$$\alpha_i = \beta_{i-1} - \gamma_d\beta_i, \qquad i = 0, 1, \ldots, d-1,$$

with

$$\beta_{-1} = 0, \qquad \beta_{d-1} = 1.$$

Writing $c = |\gamma_d|$, we get

$$\begin{aligned} |\alpha_i|^2 &\geq (c|\beta_i|^2 - |\beta_{i-1}|)^2 = c^2|\beta_i|^2 + |\beta_{i-1}|^2 - 2c|\beta_{i-1}\beta_i| \\ &\geq c^2|\beta_i|^2 + |\beta_{i-1}|^2 - c(|\beta_i|^2 + |\beta_{i-1}|^2) \\ &= (c^2 - c)|\beta_i|^2 - (c-1)|\beta_{i-1}|^2, \end{aligned}$$

and, summing over i,

$$\begin{aligned} 1 + \sum_{i=0}^{d-1} |\alpha_i|^2 \geq 1 + c^2 - c + (c^2 - c)\sum_{i=0}^{d-2}|\beta_i|^2 - (c-1)\sum_{i=0}^{d-2}|\beta_i|^2 \\ = (c-1)^2\sum_{i=0}^{d-2}|\beta_i|^2 + c^2 - c + 1 \\ = (c-1)^2\{1 + \sum_{i=0}^{d-2}|\beta_i|^2\} + c, \end{aligned}$$

so that

$$|P|_v > (c-1)|Q|_v$$

and

$$|Q|_v < \frac{1}{c-1}|P|_v.$$

By induction,

$$\prod_{i=1}^{d-1}(1 + |\gamma_i|_v^2)^{1/2} \leqq 5^{(d-1)/2}|Q|_v$$

so that

$$\begin{aligned} \prod_{i=1}^{d}(1 + |\gamma_i|_v^2)^{1/2} &< (1 + c^2)^{1/2}5^{(d-1)/2}\frac{1}{c-1}|P|_v \\ &\leqq 5^{d/2}|P|_v, \end{aligned}$$

since $c \geqq 2$.

LEMMA 7C. *Given n, d and B, there are only finitely many non-zero vectors ($\underline{\underline{\alpha}} = (\alpha_1, \ldots, \alpha_n)$ with each α_i of degree $\leqq d$ and $H(\underline{\underline{\alpha}}) \leqq B$, if you consider proportional vectors the same.*

Proof. Without loss of generality, consider vectors $(1, \alpha_2, \ldots, \alpha_n)$. Then

$$H_K(1, \alpha_2, \ldots, \alpha_n) \geqq H_K(1, \alpha_i) = h_K(\alpha_i) \quad (i = 2, \ldots, n),$$

since $|(1, \alpha_2, \ldots, \alpha_n)|_v \geqq |(1, \alpha_i)|_v$. Thus it suffices to show there are only finitely many α of given degree d with $h(\alpha) \leqq B$. Such α would satisfy a polynomial equation $P(\alpha) = 0$ where

$$P(X) = (X - \alpha^{(1)})(X - \alpha^{(2)}) \cdots (X - \alpha^{(d)})$$

with $\alpha^{(1)}, \ldots, \alpha^{(d)}$ the conjugates of α. Here P has rational coefficients. Then

$$\begin{aligned} H(P) &\leqq 2^{(d-1)/2} h(\alpha^{(1)}) \cdots h(\alpha^{(d)}) \\ &\leqq 2^{(d-1)/2} B^d \end{aligned}$$

since $h(\alpha^{(1)}) = \cdots = h(\alpha^{(d)})$ and $h(\alpha) \leqq B$. There are only finitely many such polynomials P. Because suppose $P(X) = X^d + \rho_{d-1}X^{d-1} + \cdots + \rho_0$ where $\rho_i \in \mathbb{Q}$ $(i = 0, \ldots, d-1)$. If $H(P) = H(1, \rho_{d-1}, \ldots, \rho_0) \leqq 2^{(d-1)/2}B^d$, then $H(1, \rho_i) \leqq 2^{(d-1)/2}B^d$ $(i = 0, \ldots, d-1)$, and clearly there are only finitely many such rational $\rho_0, \ldots, \rho_{d-1}$.

Open Problem. Given n, d, and B, find an asymptotic formula for the number of vectors $\underline{\underline{\alpha}}$ satisfying the hypothesis of Lemma 7C.

For $\alpha \in K$ and $v \in M(K)$, we define

$$\langle \alpha \rangle_v = |\alpha|_v^{n_v}.$$

Then the product formula becomes

$$\prod_{v \in M(K)} \langle \alpha \rangle_v = 1$$

for $\alpha \neq 0$ in K.

LEMMA 7D. *If $\alpha_1 \neq \alpha_2$ in K, then for any $v \in M(K)$,*

$$\langle \alpha_1 - \alpha_2 \rangle_v = |\alpha_1 - \alpha_2|_v^{n_v} \geqq \frac{1}{h_K(\alpha_1) h_K(\alpha_2)}.$$

Proof. If v is non-Archimedean, then

$$\begin{aligned} |\alpha_1 - \alpha_2|_v &\leqq \max(|\alpha_1|_v, |\alpha_2|_v) \\ &\leqq (\max(1, |\alpha_1|_v))(\max(1, |\alpha_2|_v)). \end{aligned}$$

If v is Archimedean, then

$$|\alpha_1 - \alpha_2|_v \leqq \sqrt{1 + |\alpha_1|_v^2}\,\sqrt{1 + |\alpha_2|_v^2},$$

which follows easily by considering α_1, α_2 as complex numbers and $|\ |_v$ as the usual absolute value on $\mathbb{C}$. Then the product formula gives

$$\begin{aligned} 1 &= \prod_{w \in M(K)} |\alpha_1 - \alpha_2|_w^{n_w} \\ &= |\alpha_1 - \alpha_2|_v^{n_v} \prod_{\substack{w \in M(K) \\ w \neq v}} |\alpha_1 - \alpha_2|_w^{n_w} \\ &\leqq |\alpha_1 - \alpha_2|_v^{n_v} \prod_{w \in M(K)} |(1, \alpha_1)|_w^{n_w} |(1, \alpha_2)|_2^{n_w} \\ &= |\alpha_1 - \alpha_2|_v^{n_v} h_K(\alpha_1) h_K(\alpha_2), \end{aligned}$$

and the result follows.

§8. Heights of Subspaces.

Let K be an algebraic number field and S^p a subspace of dimension p spanned by $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p$. Then the Grassman coordinates of S^p are given by $\underline{\underline{X}} = \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p$. We define the *field height* of S^p by

$$H_K(S^p) = H_K(\underline{\underline{X}})$$

and the *absolute height* by

$$H(S^p) = H(\underline{\underline{X}}).$$

When $p = 0$, so that $S^0 = \{\underline{\underline{0}}\}$, put $H_K(S^0) = H(S^0) = 1$. ¿From Lemma 5G, we have for $0 < p < n$ that

$$H(S^p) = H((S^p)^\perp).$$

Since K_n^n is a 1–dimensional vector space, it is clear that $H(K^n) = 1$. Therefore the above relation holds for $p = 0$ or $p = n$ also.

LEMMA 8A. *If $S, T \subseteq K^n$ are subspaces and $S + T$ is the subspace of vectors $\underline{\underline{s}} + \underline{\underline{t}}$ where $\underline{\underline{s}} \in S$, $\underline{\underline{t}} \in T$, then*

$$H(S \cap T) H(S + T) \leqq H(S) H(T).$$

Proof. Let $U = S \cap T$. Pick a basis $\underline{\underline{u}}_1, \dots, \underline{\underline{u}}_\ell$ of U. Then we can choose a basis $\underline{\underline{u}}_1, \dots, \underline{\underline{u}}_\ell, \underline{\underline{x}}_1, \dots, \underline{\underline{x}}_p$ for S and a basis $\underline{\underline{u}}_1, \dots, \underline{\underline{u}}_\ell, \underline{\underline{y}}_1, \dots, \underline{\underline{y}}_q$ for T. All we need to show is that

$$\begin{aligned} &|\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell|_v |\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell \wedge \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|_v \\ &\leqq |\underline{\underline{u}}_1 \wedge \cdots \wedge \underline{\underline{u}}_\ell \wedge \underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p|_v \, |\underline{\underline{u}}_1, \dots, \underline{\underline{u}}_\ell \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|_v \end{aligned}$$

for every $v \in M(K)$. We have already proven the Archimedean case. (See Lemma 5F.) The non-Archimedean case is left to the reader.

Exercise 8a. Prove the inequality above for v non-Archimedean. (When $\ell = 0$, the above inequality is to be interpreted as $|\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p \wedge \underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|_v \leqq |\underline{\underline{x}}_1 \wedge \cdots \wedge \underline{\underline{x}}_p|_v |\underline{\underline{y}}_1 \wedge \cdots \wedge \underline{\underline{y}}_q|_v$.)

For $B \in \mathbb{Z}$ with $B > 0$, let $N(K, n, p, B)$ denote the number of p–dimensional subspaces S^p of K^n with $H_K(S^p) \leqq B$. Then $N(K, n, p, B)$ is bounded. W. M. Schmidt showed (1967) that

$$N(K, n, p, B) \gg\ll B^n \tag{8.1}$$

where the notation $\gg\ll$ means there exist constants C, C' such that

$$C'(K, n, p)B^n \leqq N(K, n, p, B) \leqq C(K, n, p)B^n.$$

Notice that the constants C, C' may depend on K, n, and p. Schmidt (1968) also showed that in the special case $K = \mathbb{Q}$, we have the asymptotic relationship

$$N(\mathbb{Q}, n, p, B) \sim c_0(n, p)B^n$$

for $0 < p < n$. Here

$$c_0(n, p) = \frac{1}{n}\binom{n}{p} \frac{V(n)V(n-1)\cdots V(n-p+1)}{V(1)V(2)\cdots V(p)} \frac{\zeta(2)\zeta(3)\cdots\zeta(p)}{\zeta(n)\zeta(n-1)\cdots\zeta(n-p+1)}$$

where $V(n)$ denotes the volume of the unit ball in $\mathbb{R}^n$. Notice that $c_0(n, p) = c_0(n, n - p)$. In general, (i.e., for K an arbitrary number field), an asymptotic formula was recently derived by J. Thunder (to appear). Schanuel (1979) has given such a formula for $N(K, n, 1, B)$, but for different heights.

LEMMA 8B. *Let K be an algebraic number field of degree d and $\theta \neq 0$ an algebraic number which is not necessarily in K. Given $B \geqq 1$, the number of α's in K satisfying*

$$h(\alpha\theta) \leqq B$$

is bounded by

$$36(2B)^{2d}.$$

A similar result is due to Evertse (1984).

Remark. Consider the case $\theta = 1$. For $\alpha \in K$, the condition $h(\alpha) \leqq B$ can be written as $H_K(1, \alpha) \leqq B^d$ since $(h(\alpha))^d = h_K(\alpha) = H_K(1, \alpha)$. Lemma 8B agrees with (8.1), according to which the number of pairs $(1, \alpha)$ satisfying the last inequality has order of magnitude B^{2d}.

Proof. For $\alpha \in K$, we will use the notation $\langle\alpha\rangle_v = |\alpha|_v^{n_v}$ and the corresponding product formula

$$\prod_{v \in M(K)} \langle\alpha\rangle_v = 1.$$

For $\underline{\underline{\beta}} \in K^n$ we will let $\langle \underline{\underline{\beta}} \rangle_v = |\underline{\underline{\beta}}|_v^{n_v}$ so that

$$H_K(\underline{\underline{\beta}}) = \prod_{v \in M(K)} \langle \underline{\underline{\beta}} \rangle_v .$$

Let L be a field containing K and θ. For $v \in M(K)$, we have

$$\langle \alpha \rangle_v = |\alpha|_v^{n_v} = \prod_{\substack{w \in M(L) \\ w|v}} (|\alpha|_w^{n_w})^{1/[L:K]}$$

since the exponent on the right-hand side is (see (v) of §6)

$$\sum_{\substack{w \in M(L) \\ w|v}} \frac{n_w}{[L:K]} = n_v .$$

In our new notation,

$$\langle \alpha \rangle_v = \prod_{\substack{w \in M(L) \\ w|v}} \langle \alpha \rangle_w^{1/[L:K]} \tag{8.2}$$

Fix an Archimedean $v \in M(K)$. Assume, say, that v corresponds to a complex embedding of K into $\mathbb{C}$. Consider

$$\begin{aligned} h_L(\alpha\theta) &= \prod_{w \in M(L)} \langle (1, \alpha\theta) \rangle_w \\ &= h_{L1}(\alpha\theta) h_{L2}(\alpha\theta) \end{aligned}$$

where

$$h_{L1}(\alpha\theta) = \prod_{\substack{w \in M(L) \\ w|v}} \langle (1, \alpha\theta) \rangle_w \quad \text{and} \quad h_{L2}(\alpha\theta) = \prod_{\substack{w \in M(L) \\ w|v}} \langle (1, \alpha\theta) \rangle_{\mathbf{w}}$$

Then

$$h(\alpha\theta) = h_1(\alpha\theta) h_2(\alpha\theta)$$

where $h_i(\alpha\theta) = h_{Li}(\alpha\theta)^{1/[L:\mathbb{Q}]}$ $(i = 1, 2)$. We will initially estimate the number of α's in K satisfying $h_1(\alpha\theta) \leqq B_1$ and $h_2(\alpha\theta) \leqq B_2$.

Take such an α. Then

$$\begin{aligned} \langle \alpha \rangle_v &= \prod_{\substack{w \in M(L) \\ w|v}} \langle \alpha \rangle_w^{1/[L:K]} \quad \text{(by (8.2))} \\ &= \prod_{\substack{w \in M(L) \\ w|v}} \langle \alpha\theta \rangle_w^{1/[L:K]} M_v^{-d} \end{aligned}$$

where

$$M_v = \prod_{\substack{w \in M(L) \\ w|v}} \langle \theta \rangle_w^{1/[L:\mathbb{Q}]} .$$

Then

$$\begin{aligned}\langle\alpha\rangle_v &\leqq h_{L1}(\alpha\theta)^{1/[L:K]}M_v^{-d}\\ &= (h_1(\alpha\theta)/M_v)^d\\ &\leqq (B_1/M_v)^d\end{aligned}$$

where the first inequality follows because $\langle\alpha\theta\rangle_w \leqq \langle(1,\alpha\theta)\rangle_w$ for each w. The assumption that v corresponds to a complex embedding gives

$$|\alpha|_v \leqq (B_1/M_v)^{d/2}$$

since $\langle\alpha\rangle_v = |\alpha|_v^2$. So α lies in a square centered at the origin with sides of length $2(B_1/M_v)^{d/2}$.

Suppose there are N elements α satisfying the inequalities $h_1(\alpha\theta) \leqq B_1$, $h_2(\alpha\theta) \leqq B_2$. Assume that $N \geqq 2$. Pick the positive integer t satisfying

$$t^2 < N \leqq (t+1)^2.$$

Divide the original square into t^2 squares of equal size. Since $N > t^2$, there exist $\alpha_1 \neq \alpha_2$ satisfying the two inequalities and lying in the same subsquare. Then

$$\begin{aligned}|\alpha_1-\alpha_2|_v &\leqq \frac{2\sqrt{2}}{t}(B_1/M_v)^{d/2}\\ &< \frac{3}{t}(B_1/M_v)^{d/2}\end{aligned}$$

and

$$\begin{aligned}\langle\alpha_1-\alpha_2\rangle_v &< \frac{9}{t^2}(B_1/M_v)^d\\ &\leqq \frac{36}{N}(B_1/M_v)^d.\end{aligned} \tag{8.3}$$

In the case where v corresponds to a real embedding, the same bound can be derived.

Since $\theta(\alpha_1-\alpha_2)$ is non-zero, the product formula holds. Consider first the factor

$$\begin{aligned}\prod_{\substack{w\in M(L)\\ w|v}} \langle\theta\rangle_w\langle\alpha_1-\alpha_2\rangle_w &= M_v^{[L:\mathbb{Q}]}\langle\alpha_1-\alpha_2\rangle_v^{[L:K]}\\ &\leqq 36^{[L:K]}B_1^{[L:\mathbb{Q}]}N^{-[L:K]} \quad \text{(by (8.3))}\\ &= (36B_1^dN^{-1})^{[L:K]}.\end{aligned}$$

The remaining factor is

$$\prod_{\substack{w\in M(L)\\ w|v}} \langle\theta\alpha_1-\theta\alpha_2\rangle_w.$$

Using the fact that

$$|\theta\alpha_1-\theta\alpha_2|_w \leqq \begin{cases}\max(1,|\theta\alpha_1|_w)\max(1,|\theta\alpha_2|_w) & \text{if } w \text{ is non-Archimedean,}\\ \sqrt{1+|\theta\alpha_1|_w^2}\,\sqrt{1+|\theta\alpha_2|_w^2} & \text{if } w \text{ is Archimedean,}\end{cases}$$

we have

$$\begin{aligned}\prod_{\substack{w\in M(L)\\ w\mid v}} \langle \theta\alpha_1-\theta\alpha_2\rangle_w &\leqq \prod_{\substack{w\in M(L)\\ w\mid v}} \langle(1,\theta\alpha_1)\rangle_w\langle(1,\theta\alpha_2)\rangle_w\\ &\leqq h_{L2}(\theta\alpha_1)h_{L2}(\theta\alpha_2)\\ &=(h_2(\theta\alpha_1)h_2(\theta\alpha_2))^{[L:K]\cdot d}\\ &\leqq (B_2^{2d})^{[L:K]}.\end{aligned}$$

Then the product formula gives

$$1 \leqq (36\cdot B_1^dB_2^{2d}N^{-1})^{[L:K]}$$

and

$$N \leqq 36\cdot B_1^dB_2^{2d}. \tag{8.4}$$

This is trivially true when $N<2$. Recall that N was the number of $\alpha\in K$ with $h_1(\alpha\theta)\leqq B_1$, $h_2(\alpha\theta)\leqq B_2$.

We now complete the proof of the lemma as follows. Given α with $h(\alpha\theta)=h_1(\alpha\theta)h_2(\alpha\theta)\leqq B$, let k be the integer with

$$2^{k-1}\leqq h_1(\alpha\theta)<2^k.$$

Then $k\geqq 1$ and $2^{k-1}\leqq B$ so that

$$h_2(\alpha\theta)\leqq B\cdot 2^{1-k}.$$

Given k, the number of corresponding $\alpha\in K$ is (by (8.4) with $B_1=2^k$, $B_2=B\cdot 2^{1-k}$)

$$\begin{aligned}&\leqq 36\cdot 2^{kd}B^{2d}2^{2d-2kd}\\ &=36\cdot 2^{2d}B^{2d}2^{-kd}.\end{aligned}$$

Summing over all $k\geqq 1$, the total number of α's is

$$\leqq 36\cdot 2^{2d}B^{2d}.$$

§9. Another Version of Siegel's Lemma.

Let K be a number field of degree d with embeddings $\sigma_1,\dots,\sigma_d$ into $\mathbb{C}$. Given $\underline{\underline{\alpha}}_1,\dots,\underline{\underline{\alpha}}_m$ in K^n, let S be the subspace of K^n which they span. We have $\underline{\underline{\alpha}}_1^{(i)},\dots,\underline{\underline{\alpha}}_m^{(i)}$ in $K^{(i)}$ $(i=1,\dots,d)$, where σ_i is the isomorphism $K\to K^{(i)}$. Let $\hat{K}$ denote the compositum of $K^{(1)},\dots,K^{(d)}$, and $\hat{S}$ the subspace of $\hat{K}$ spanned by $\underline{\underline{\alpha}}_1^{(1)},\dots,\underline{\underline{\alpha}}_m^{(1)},\dots,\underline{\underline{\alpha}}_1^{(d)},\dots,\underline{\underline{\alpha}}_m^{(d)}$. If $\hat{m}=\dim\hat{S}$, then $\hat{m}\leqq md$. Let $w_1,\dots,w_d$ be a field basis for $K/\mathbb{Q}$, so that each $\underline{\underline{\alpha}}_j$ has the form

$$\underline{\underline{\alpha}}_j=w_1\underline{\underline{x}}_{j1}+\cdots+w_d\underline{\underline{x}}_{jd} \qquad (1\leqq j\leqq m)$$

with $\underline{\underline{x}}_{j\ell} \in \mathbb{Q}^n$ $(1 \leqq \ell \leqq d)$. Then

$$\underline{\underline{\alpha}}_j^{(i)} = w_1^{(i)}\underline{\underline{x}}_{j1} + \cdots + w_d^{(i)}\underline{\underline{x}}_{jd} \quad (1 \leqq j \leqq m,\ 1 \leqq i \leqq d).$$

The matrix $(w_\ell^{(i)})$ is non-singular. For fixed j, each vector $\underline{\underline{x}}_{j\ell}$ $(1 \leqq \ell \leqq d)$ is a linear combination of $\underline{\underline{\alpha}}_j^{(1)}, \dots, \underline{\underline{\alpha}}_j^{(d)}$. So $\hat{S}$ is spanned by $\underline{\underline{x}}_{j\ell}$ $(1 \leqq j \leqq m,\ 1 \leqq \ell \leqq d)$, and $\hat{S}$ is defined over $\mathbb{Q}$ (i.e., $\hat{S}$ is spanned by vectors with rational components).

The orthogonal complement $\hat{S}^\perp$ is also defined over $I\mathbb{Q}$ and

$$\dim \hat{S}^\perp = n - \hat{m} \geqq n - md.$$

Assume now that $n > md$. By Lemma 4B, there exists an integer point $\underline{\underline{x}} \neq \underline{\underline{0}}$ in $\hat{S}^\perp$ with

$$\begin{aligned} \overline{|\underline{\underline{x}}|} &\leqq H(\hat{S}^\perp)^{1/(n-\hat{m})} \\ &\leqq H(\hat{S}^\perp)^{1/(n-md)} \\ &= H(\hat{S})^{1/(n-md)}. \end{aligned}$$

Let $S^{(i)}$ $(1 \leqq i \leqq d)$ denote the subspace spanned by $\underline{\underline{\alpha}}_1^{(i)}, \dots, \underline{\underline{\alpha}}_m^{(i)}$ and S again the space spanned by $\underline{\underline{\alpha}}_1, \dots \underline{\underline{\alpha}}_m$. Then $\hat{S} = S^{(1)} \oplus \cdots \oplus S^{(d)}$ and

$$\begin{aligned} H(\hat{S}) &\leqq H(S^{(1)}) \cdots H(S^{(d)}) && \text{(by Lemma 8A)} \\ &= H(S)^d && \text{(by (vii) of §6)} \\ &\leqq (H(\underline{\underline{\alpha}}_1) \cdots H(\underline{\underline{\alpha}}_m))^d && \text{(by Lemma 8A)} \end{aligned}$$

We have proven the following version of Siegel's Lemma:

LEMMA 9A. *Suppose K is a number field of degree d, the vectors $\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_m$ in K^n span a subspace S, and $dm < n$. Then there is a vector $\underline{\underline{x}} \in \mathbb{Z}^n \backslash \underline{\underline{0}}$ with*

$$\underline{\underline{\alpha}}_j \underline{\underline{x}} = 0 \qquad (j = 1, \dots, m)$$

and

$$\begin{aligned} \overline{|\underline{\underline{x}}|} &\leqq H(S)^{d/(n-md)} \\ &\leqq (H(\underline{\underline{\alpha}}_1) \cdots H(\underline{\underline{\alpha}}_m))^{d/(n-md)}. \end{aligned}$$

This particular formulation is due to Bombieri and Vaaler (1983). They assumed, however, that $S^{(1)} \oplus \cdots \oplus S^{(d)}$ had dimension md.

Remark. In fact, there are $n - dm$ linearly independent solutions $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_{n-dm}$ such that

$$\begin{aligned} \overline{|\underline{\underline{x}}_1|} \cdots \overline{|\underline{\underline{x}}_{n-dm}|} &\leqq H(S)^d \\ &\leqq (H(\underline{\underline{\alpha}}_1) \cdots H(\underline{\underline{\alpha}}_m))^d. \end{aligned}$$

More generally, Bombieri and Vaaler consider a number field $k \subset K$ and a system of equations $\underline{\underline{\alpha}}_i \underline{\underline{x}} = 0$ $(i = 1, \dots, m)$ where $\underline{\underline{\alpha}}_i \in K^n$, and they seek solutions $\underline{\underline{x}} \in k^n$.

II. Diophantine Approximation

References: Cassels (1957), Schmidt (1980).

§1. Dirichlet's Theorem and Liouville's Theorem.

THEOREM 1A. (Dirichlet, (1842)) *Given $\alpha \in \mathbb{R}$ and $N > 1$, there exist integers x, y with $1 \leqq y \leqq N$ and*

$$|\alpha y - x| < 1/N.$$

When α is irrational, there are infinitely many reduced fractions x/y with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2}.$$

Remark. It is clear that the first statement remains true when we require that x, y be relatively prime. Then the second inequality follows by

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{Ny} \leqq \frac{1}{y^2}.$$

Since α is irrational, $\alpha y - x$ is never zero, thus for fixed x, y the inequality $|\alpha y - x| < 1/N$ can be satisfied only for N under a fixed bound. Then as $N \to \infty$, we must get infinitely many distinct pairs x, y.

THEOREM 1B. (Dirichlet) *Given $\alpha_1, \ldots, \alpha_n$ in R and $N > 1$, there exist $y, x_1, \ldots, x_n$ in $\mathbb{Z}$ with $1 \leqq y \leqq N$ and*

$$|\alpha_i y - x_i| < N^{-1/n} \quad (i = 1, \ldots, n).$$

If at least one of the $\alpha_1, \ldots, \alpha_n$ is irrational, then there are infinitely many n–tuples $\left(\frac{x_1}{y}, \ldots, \frac{x_n}{y}\right)$ with $gcd(y, x_1, \ldots x_n) = 1$ and

$$\left|\alpha_i - \frac{x_i}{y}\right| < \frac{1}{y^{1+(1/n)}} \qquad (i = 1, \ldots, n).$$

Consider the system of inequalities:

$$\begin{aligned} |\alpha_{11}x_1 + \cdots + \alpha_{1n}x_n| &< A_1 \\ &\vdots \\ |\alpha_{n-1,1}x_1 + \cdots + \alpha_{n-1,n}x_n| &< A_{n-1} \\ |\alpha_{n1}x_1 + \cdots + \alpha_{nn}x_n| &\leqq A_n \end{aligned} \tag{1.1}$$

where $|\det(\alpha_{ij})| \neq 0$ and $A_i > 0$ $(i = 1, \ldots, n)$. This system defines a parallelepiped of volume

$$\frac{2^n A_1 \cdots A_n}{|\det(\alpha_{ij})|}. \tag{1.2}$$

Suppose $A_1 \cdots A_n \geqq |\det(\alpha_{ij})|$. Then the volume of the parallelepiped is greater than or equal to 2^n, and the result would follow by Minkowski's Theorem (2C) of Chapter I *if* we had a compact set. However, we have

LEMMA 1C. *Suppose $A_i > 0$ $(i = 1, \dots, n)$ and $A_1 \cdots A_n \geqq |\det(a_{ij})| > 0$ in (1.1). Then the system of inequalities has a solution $\underline{\underline{x}} \in \mathbb{Z}^n \backslash \underline{\underline{0}}$.*

Exercise 1a. Prove Lemma 1C.

Proof (of Theorem 1B). In $\mathbb{R}^{n+1}$, consider the system of inequalities

$$\begin{aligned} &|\alpha_1 y - x_1| < N^{-1/n} \\ &\quad\vdots \\ &|\alpha_n y - x_n| < N^{-1/n} \\ &|y| \leqq N. \end{aligned}$$

By Lemma 1C, there is a non-trivial solution. If we had $y = 0$, then $x_1, \dots, x_n$ would all be zero, too. Thus $y \neq 0$. Then there exists a solution with $y > 0$, therefore $1 \leqq y \leqq N$. The second assertion of Theorem 1B follows just like in Theorem 1A.

Theorem 1A was improved by Hurwitz (1891). He showed, for α irrational, that there exist infinitely many fractions x/y with

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{\sqrt{5}\, y^2}.$$

See, e.g., Schmidt (1980) for a proof. The following Lemma can be used to show that the constant $\sqrt{5}$ is best possible.

LEMMA 1D. *Suppose α is a real quadratic irrational satisfying $a\alpha^2 + b\alpha + c = 0$ with $a, b, c \in \mathbb{Z}$, the leading coefficient $a > 0$ and discriminant $D = b^2 - 4ac$. Then for $A > \sqrt{D}$, there are only finitely many fractions x/y with*

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{Ay^2}.$$

Example. Consider the polynomial equation $\alpha^2 - \alpha - 1 = 0$. Here $D = 5$ and $\alpha = (1 + \sqrt{5})/2$. Using Lemma 1D, we see that for $A > \sqrt{5}$ there are only finitely many solutions to $|\alpha - (x/y)| < 1/(Ay^2)$. Thus Hurwitz's result is best possible.

Proof. Writing $f(X) = aX^2 + bX + c = a(X-\alpha)(X-\alpha')$ gives $D = a^2(\alpha-\alpha')^2$. Then if $|\alpha - (x/y)| < 1/(Ay^2)$, we have

$$\begin{aligned}\frac{1}{y^2} &\leqq \left|f\left(\frac{x}{y}\right)\right| \\ &= \left|a\left(\frac{x}{y}-\alpha\right)\left(\frac{x}{y}-\alpha'\right)\right| \\ &< \frac{a}{Ay^2}\left|\alpha-\alpha'+\frac{x}{y}-\alpha\right| \\ &< \frac{\sqrt{D}}{Ay^2}+\frac{a}{A^2y^4}.\end{aligned}$$

Subtracting $\sqrt{D}/Ay^2$ from both sides gives

$$\frac{1}{y^2}\left(1-\frac{\sqrt{D}}{A}\right) < \frac{a}{A^2y^4},$$

which becomes

$$y^2 < \frac{a}{a(A-\sqrt{D})}.$$

The result is proven.

Given any quadratic irrationality α, there exists a $c > 0$ such that

$$\left|\alpha - \frac{x}{y}\right| \geqq \frac{c}{y^2}$$

for any $\frac{x}{y} \neq \alpha$. Any irrational α satisfying

$$\left|\alpha - \frac{x}{y}\right| \geqq \frac{c(\alpha)}{y^2}$$

for some constant $c(\alpha) > 0$ is called *badly approximable.*

THEOREM 1E. (Liouville (1844).) *Suppose α is algebraic of degree d. Then there exists a constant $c(\alpha) > 0$ such that for any rational $\frac{x}{y} \neq \alpha$, we have*

$$\left|\alpha - \frac{x}{y}\right| > \frac{c(\alpha)}{y^d}.$$

Proof. The proof is broken into three steps which will be important in a more general context later on.

(a) Let $P(X)$ be the defining polynomial of α. So $\deg P = d$, the coefficients of P are in $\mathbb{Z}$ (i.e., $P(X) \in \mathbb{Z}[X]$), and $P(\alpha) = 0$.

(b) For rational $\frac{x}{y} \neq \alpha$, we have

$$\left|P\left(\frac{x}{y}\right)\right| \geqq \frac{1}{y^d}.$$

(c) Expanding P into a Taylor series at α, we get

$$P\left(\frac{x}{y}\right) = \sum_{i=1}^{d}\left(\frac{x}{y} - \alpha\right)^{i} \frac{P^{(i)}(\alpha)}{i!},$$

since $P(\alpha) = 0$. We may assume that

$$\left|\alpha - \frac{x}{y}\right| \leqq 1.$$

(Otherwise, we're done.) Then

$$\frac{1}{y^d} \leqq \left|P\left(\frac{x}{y}\right)\right| \leqq \left|\alpha - \frac{x}{y}\right| \sum_{i=1}^{d} \frac{|P^{(i)}(\alpha)|}{i!}.$$

Let $c(\alpha)$ be defined by

$$\sum_{i=1}^{d} \frac{|P^{(i)}(\alpha)|}{i!} = \frac{1}{2c(\alpha)};$$

then the result follows.

COROLLARY 1F. (Liouville) *The number* $\alpha = \sum_{\nu=1}^{\infty} 2^{-\nu!}$ *is transcendental.*

Liouville was first to exhibit transcendental numbers, in fact first to prove the existence of such numbers.

Proof. Write $y(k) = 2^{k!}$ and $x(k) = 2^{k!}\sum_{\nu=1}^{k} 2^{-\nu!}$. Then $x(k), y(k) \in \mathbb{Z}$ $(k \geqq 1)$ and

$$\begin{aligned}\alpha - \frac{x(k)}{y(k)} &= \sum_{\nu=k+1}^{\infty} 2^{-\nu!}\\ &= 2^{-(k+1)!} + \cdots\\ &< 2 \cdot 2^{-(k+1)!}\\ &= 2/y(k+1)\\ &< c/y(k)^d\end{aligned}$$

for any given c, d, provided that $k > k_0(c,d)$. Hence, for any d, we have α not algebraic of degree d by Liouville's Theorem (1E).

The numbers which can be proved transcendental by Liouville's Theorem are called "Liouville numbers". They form a set of measure zero. This explains why Liouville's Theorem is not enough to prove the transcendence of classical numbers such as e or π.

Exercise 1b. Given $\alpha \in \mathbb{R}$ and $N > 0$, there exist $x, y \in \mathbb{Z}$, not both 0, with

$$N|\alpha y - x| + N^{-1}|y| \leqq \sqrt{2}.$$

Now use the arithmetic–geometric inequality to show that given $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, there are infinitely many rationals $\frac{x}{y}$ with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{2y^2}.$$

(This is better than Dirichlet's Theorem, but worse than Hurwitz's Theorem.)

§2. Roth's Theorem.

A consequence of Liouville's Theorem is the following: If $\deg \alpha = d \geqq 2$ and $\mu > d$, then

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^\mu}$$

has only finitely many solutions $\frac{x}{y}$. Thue (1908) strengthened this result by weakening the hypothesis to $\mu > (d/2) + 1$. Siegel (1921) in his thesis improved this to $\mu > 2\sqrt{d}$. Dyson (1947) and Gelfond (1952) showed that the result holds for $\mu > \sqrt{2d}$. In 1956, Roth received a Field prize for his 1955 result with $\mu > 2$. Dirichlet's Theorem shows that Roth's result is best possible.

THEOREM 2A. (Roth (1955).) *If α is algebraic and $\delta > 0$, there are only finitely many rationals $\frac{x}{y}$ with*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}}.$$

Remarks.

(i) Roth's result is correct but trivial for $\alpha \in \mathbb{C}\backslash\mathbb{R}$.
(ii) If $\deg \alpha = 2$, then Lemma 1D is better.
(iii) We know that there are infinitely many $\frac{x}{y}$ with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2},$$

and only finitely many $\frac{x}{y}$ with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}}$$

with $\delta > 0$. For any given α with deg $\alpha \geqq 3$, it is still unknown whether α is badly approximable, i.e. whether there exists a $c > 0$ so that

$$\left|\alpha - \frac{x}{y}\right| > \frac{c}{y^2}$$

for every rational $\frac{x}{y}$. The conjecture is that this holds for no algebraic α of degree $\geqq 3$.

(iv) Another conjecture is that Roth's Theorem holds in the following strengthened form: *the inequality*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2(\log y)^k}$$

has only finitely many solutions for $k > 1$.

The following theorem gives heuristic grounds for the conjectures in (iii) and (iv).

THEOREM 2B. (Khintchine (1926).) *Suppose* $\psi(y) > 0$ *is defined on the positive integers and* ψ *is nonincreasing. Consider the inequality*

$$\left|\alpha - \frac{x}{y}\right| < \frac{\psi(y)}{y}. \tag{2.1}$$

If

(i) $\sum_{y=1}^{\infty} \psi(y) < \infty$, *then (2.1) has only finitely many solutions for almost all* α.

(ii) $\sum_{y=1}^{\infty} \psi(y) = \infty$, *then (2.1) has infinitely many solutions for almost all* α.

Remarks. Take $\psi(y) = 1/y(\log y)^k$ with $k > 1$. Then case (i) in Kintchine's Theorem says that

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2(\log y)^k}$$

has only finitely many solutions for almost all α. Taking $\psi(y) = 1/y \log y$, case (ii) tells us that

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2 \log y}$$

has infinitely many solutions for almost all α.

Here we will only prove the easy part (i) of Khintchine's Theorem. The inequality (2.1) defines an interval for α of length $2\psi(y)/y$. The union of these intervals for $x = 1, 2, \dots, y$ has measure $\leqq 2\psi(y)$. The union of the intervals (2.1) with $x \in \mathbb{Z}$ is a set which is invariant under translations by integers, and the intersection of this set with $0 \leqq \alpha < 1$ has measure $\leqq 2\psi(y)$. Thus if $S(y)$ is the set of numbers α in $0 \leqq \alpha < 1$ for which (2.1) holds for some x, then $S(y)$ has measure $\mu(S(y)) \leqq 2\psi(y)$. Further if

$$S_N = \bigcup_{y=N}^{\infty} S(y),$$

then $\mu(S_N) \to 0$ since $\sum_{y=1}^{N} \psi(y)$ is convergent. Now α in $0 \leqq \alpha < 1$ has infinitely many solutions to (2.1) precisely when α lies in

$$\bigcap_{N=1}^{\infty} S_N;$$

but this set has measure 0.

Outline of Proof of Roth's Theorem. We might try the following.

(a) Pick a polynomial $P(X) \in \mathbb{Z}[X]$ which is not identically zero, vanishes at α of order q, and has degree r.

(b) Show that $P\left(\frac{x}{y}\right) \neq 0$ with only finitely many exceptions $\frac{x}{y}$. Then

$$\left|P\left(\frac{x}{y}\right)\right| \geqq \frac{1}{y^r}.$$

(c) Consider the Taylor expansion

$$P\left(\frac{x}{y}\right) = \sum_{i=q}^{r} \left(\frac{x}{y} - \alpha\right)^i \frac{P^{(i)}(\alpha)}{i!}.$$

Then if $\left|\frac{x}{y} - \alpha\right| \leqq 1$, we have

$$\left|P\left(\frac{x}{y}\right)\right| \leqq \left|\frac{x}{y} - \alpha\right|^q \cdot C(\alpha)$$

for some constant $C(\alpha)$, so that

$$\left|\frac{x}{y} - \alpha\right| \geqq \frac{C'}{y^{r/q}}$$

with C' constant.

This is good if r/q is small. But if $\deg \alpha = d$, then $r \geqq qd$. Thus $r/q \geqq d$, and we get no improvement over Liouville's Theorem.

This argument can be modified by using a polynomial in m variables. Thue used a polynomial in 2 variables of the form $P(X_1, X_2) = X_2 Q(X_1) - P(X_1)$. Siegel used a more general polynomial in two variables, and so did Dyson and Gelfond. Only Roth was able to overcome the difficulties involved in dealing with more than 2 variables.

To see why a polynomial in m variables offers an advantage, consider $P(X_1, \dots, X_m) \in \mathbb{Z}[X_1, \dots, X_m]$ of degree at most r in each variable.[†] Such a polynomial is made up of monomials $X_1^{i_1} \cdots X_m^{i_m}$ with $0 \leqq i_1, \dots, i_m \leqq r$. The numbers of such monomials is $(r+1)^m$, so the number of possible coefficients is also $(r+1)^m \sim r^m$ as $m \to \infty$.

Try to make P vanish at $(\alpha, \dots, \alpha)$ of order q. Then

$$P^{(j_1, \dots, j_m)}(\alpha, \dots, \alpha) = 0$$

for $j_1 + \cdots + j_m \leqq q$. The number of implied linear homogeneous equations with *rational* coefficients for the coefficients of P does not exceed

$$d\binom{q+m}{m} \sim \frac{dq^m}{m!} \tag{2.2}$$

as $q \to \infty$. Roughly speaking, we can choose r, q with

$$r^m \sim dq^m/m!,$$

[†] One might be tempted to try a polynomial of bounded *total* degree, but difficulties in part (b) preclude such an approach.

or

$$r/q \sim \sqrt[m]{d/m!}\,.$$

Use the multidimensional Taylor's formula to write

$$P\left(\frac{x}{y},\dots,\frac{x}{y}\right)=\sum\left(\frac{x}{y}-\alpha\right)^{j_1}\cdots\left(\frac{x}{y}-\alpha\right)^{j_m} c(j_1,\dots,j_m)$$

where the sum is over $j_1,\dots,j_m$ with $j_1+\cdots+j_m \geqq q$. Then if things go well, in particular when $P\left(\frac{x}{y},\dots,\frac{x}{y}\right)\neq 0$, we have

$$\frac{1}{y^{rm}} \leqq \left|P\left(\frac{x}{y},\dots,\frac{x}{y}\right)\right| \ll \left|\frac{x}{y}-\alpha\right|^{q}$$

and

$$\left|\alpha-\frac{x}{y}\right| \gg \frac{c}{y^{rm/q}}$$

with $rm/q \approx c_m \cdot \sqrt[m]{d}$, where

$$c_m = m/\sqrt[m]{m!}\,. \tag{2.3}$$

So we can hope to improve Liouville's result to

$$\mu > c_m d^{1/m},$$

and this will actually be achieved in Theorem 6A below. In order to get Roth's Theorem, one further has to show that the number of conditions imposed on the auxiliary polynomial P is often less than (2.2).

The difficulty with this approach is in step (b). The zero-set of $P(X_1,\dots,X_m)$ is some algebraic manifold in $\mathbb{R}^m$, so that it is hard to show that $P\left(\frac{x}{y},\dots,\frac{x}{y}\right)\neq 0$. To overcome this difficulty, one considers instead an m–tuple $\frac{x_1}{y_1},\dots,\frac{x_m}{y_m}$ of distinct rational approximations, and tries to show that $P\left(\frac{x_1}{y_1},\dots,\frac{x_m}{y_m}\right)\neq 0$. It turns out that one needs $y_1<y_2<\cdots<y_m$ increasing rapidly.

In order to make this approach work, one needs $|\alpha-\frac{x_i}{y_i}|$ all small ($i=1,\dots m$). For example, in the case $m=2$, one needs two good approximations $\frac{x_1}{y_1},\frac{x_2}{y_2}$ with y_2 much larger than y_1. This is why just one very good approximation gives no contradiction, and the result is "ineffective" in the sense that no bound can be stated for the size of the numerators y of very good approximations.

Effective improvements of Liouville's Theorem for certain cubic irrationals were given by A. Baker (1964). Then Feldman (1971) used Baker's theory of linear forms of logarithms to give improvements for general algebraic α. These were of the type

$$\left|\alpha-\frac{x}{y}\right| > \frac{c(\alpha)}{y^{d-c_1(\alpha)}}$$

where $c(\alpha)>0$ and $c_1(\alpha)>0$ are effective. Unfortunately, $c_1(\alpha)$ so obtained is usually very small. Then further improvements for special numbers were obtained by Baker and Stewart (1988), Bombieri (1982), Bombieri and Mueller (1983), Chudnovsky (1983).

§3. Construction of a Polynomial.

We will follow Bombieri and Van der Poorten (1987). We will construct a polynomial $P(X_1, \dots X_m) \in \mathbb{Z}[X_1, \dots, X_m]$. For any such polynomial P, define $\overline{|P|}$ to be the maximum absolute value of its coefficients. If $I = (i_1, \dots, i_m)$, then let

$$P^I = \frac{1}{i_1! i_2! \cdots i_m!} \frac{\partial^{i_1 + \cdots + i_m} P}{\partial X_1^{i_1} \cdots \partial X_m^{i_m}}.$$

Then $P^I \in \mathbb{Z}[X_1, \dots, X_m]$ for $P \in \mathbb{Z}[X_1, \dots, X_m]$. If P has degree $\leqq r_i$ in the variable X_i $(i = 1, \dots, m)$, then it is easily seen that

$$\overline{|P^I|} \leqq 2^{r_1 + \cdots + r_m} \overline{|P|} = 2^r \overline{|P|} \tag{3.1}$$

with $r = r_1 + \cdots + r_m$. One similarly shows that

$$\overline{|(P^I)^J|} \leqq 3^{r_1 + \cdots + r_m} \overline{|P|} = 3^r \overline{|P|}. \tag{3.2}$$

We will say that P is of *multidegree* $\leqq R = (r_1, \dots, r_m)$ if its degree in X_i is $\leqq r_i$ $(i = 1, \dots, m)$.

Let $\underline{\underline{\alpha}} = (\alpha_1, \dots, \alpha_m)$ with real or complex coordinates and $E = (e_1, \dots, e_m)$ with natural coordinates be given. If $P(X_1, \dots, X_m) \neq 0$, the *index* of P at $\underline{\underline{\alpha}}$ with respect to E is defined to be the largest value of t such that

$$P^I(\underline{\underline{\alpha}}) = 0$$

for every $I = (i_1, \dots i_m)$ with

$$\frac{i_1}{e_1} + \cdots + \frac{i_m}{e_m} \leqq t.$$

The index of the zero polynomial is understood to be ∞. (This definition is due to Roth.)

Remarks. If $e_1 = \cdots = e_m = 1$, then the index is simply the order of vanishing of P at $\underline{\underline{\alpha}}$. The e_i's allow different weights to be given to the different variables.

Given m–tuples $I = (i_1, \dots, i_m)$ and $E = (e_1, \dots e_m)$, let

$$\frac{I}{E} = \left(\frac{i_1}{e_1}, \dots, \frac{i_m}{e_m} \right).$$

Let $\mathfrak{S}\left(t, \frac{R}{E}\right)$ denote the set of $(\xi_1, \dots, \xi_m)$ satisfying

$$0 \leqq \xi_i \leqq 1 \qquad (i = 1, \dots, m)$$

and

$$\xi_1 \frac{r_1}{e_1} + \cdots + \xi_m \frac{r_m}{e_m} \leqq t.$$

Then

$$\frac{i_1}{e_1} + \cdots + \frac{i_m}{e_m} \leqq t$$

if and only if

$$\frac{I}{R} \in \mathfrak{S}\left(t, \frac{R}{E}\right). \tag{3.3}$$

The index of P with respect to E is the largest value of t such that $P^I(\underline{\underline{\alpha}}) = 0$ for every I satisfying (3.3).

Remark. In our applications, R and E will both be the multidegree of P.

Let $W\left(t, \frac{R}{E}\right)$ denote the volume of $\mathfrak{S}\left(t, \frac{R}{E}\right)$, let $\mathfrak{S}(t) = \mathfrak{S}\left(t, \frac{R}{R}\right)$, and $W(t) = W\left(t, \frac{R}{R}\right)$ the volume of $\mathfrak{S}(t)$.

LEMMA 3A. *Suppose $\alpha_1, \dots, \alpha_m$ lie in an algebraic number field K of degree d. Suppose $t > 0$ and $dW(t) < 1$. Suppose $\varepsilon > 0$. Then if $R = (r_1, \dots, r_m)$ is large, (i.e., each $r_i \geqq c(\alpha_1, \dots, \alpha_m, t,$*

$\varepsilon)$). there exists a polynomial

$$P(X_1, \dots X_m) \in \mathbb{Z}[X_1, \dots, X_m]$$

which is not identically zero and has multidegree $\leqq R$, such that the index of P at $\underline{\underline{\alpha}} = (\alpha_1, \dots, \alpha_m)$ with respect to R is $\geqq t$, and

$$\overline{|P|} \leqq \left((4h(\alpha_1))^{r_1} \cdots (4h(\alpha_m))^{r_m}\right)^{\frac{dW(t)}{1-dW(t)}(1+\varepsilon)}.$$

Proof. Try

$$\begin{aligned} P &= \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} c(j_1, \dots, j_m) X_1^{j_1} \cdots X_m^{j_m} \\ &= \sum_J c(J) X^J, \end{aligned}$$

with $J = (j_1, \dots, j_m)$. The coefficients $c(J)$ are the "unknowns" which need to be found. The number of coefficients (i.e., unknowns) is $n = (r_1 + 1) \cdots (r_m + 1)$. We want

$$P^I(\alpha_1, \dots, \alpha_m) = 0$$

for every I with $\frac{I}{R} \in \mathfrak{S}(t)$. That is,

$$\sum_J c(J) \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} \alpha_1^{j_1 - i_1} \cdots \alpha_m^{j_m - i_m} = 0.$$

This is a system of homogeneous linear equations in n unknowns. The conditions are parametrized by I with $\frac{I}{R} \in \mathfrak{S}(t)$.

Given such an I, denote the coefficient vector of the linear condition by $\underline{\underline{\alpha}}_I$. The components of $\underline{\underline{\alpha}}_I$ are

$$\binom{j_1}{i_1} \cdots \binom{j_m}{i_m} \alpha_1^{j_1 - i_1} \cdots \alpha_m^{j_m - i_m}.$$

For $v \in M(K)$ non-Archimedean, we have

$$|\underline{\underline{\alpha}}_I|_v \leqq \max(1, |\alpha_1|_v)^{r_1} \cdots \max(1, |\alpha_m|_v)^{r_m}.$$

For $v \in M(K)$ Archimedean, each component of $\underline{\underline{\alpha}}_i$ has norm

$$\leqq 2^{r_1+\cdots+r_m} \sqrt{1+|\alpha_1|_v^2}^{\,r_1} \cdots \sqrt{1+|\alpha_m|_v^2}^{\,r_m},$$

and the number of components of $\underline{\underline{\alpha}}_I$ is $n \leqq 2^{r_1+\cdots+r_m}$. Thus for v Archimedean,

$$|\underline{\underline{\alpha}}_I|_v \leqq 4^{r_1+\cdots+r_m} \sqrt{1+|\alpha_1|_v^2}^{\,r_1} \cdots \sqrt{1+|\alpha_m|_v^2}^{\,r_m}.$$

Then

$$H_K(\underline{\underline{\alpha}}_I) \leqq 4^{(r_1+\cdots+r_m)d} h_K(\alpha_1)^{r_1} \cdots h_K(\alpha_m)^{r_m}$$

and

$$H(\underline{\underline{\alpha}}_I) \leqq (4h(\alpha_1))^{r_1} \cdots (4h(\alpha_m))^{r_m}.$$

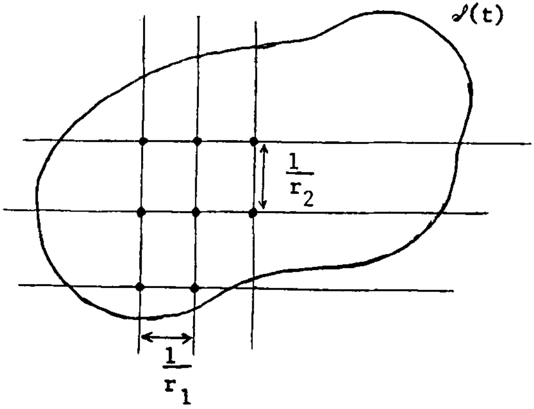
Recall, the number of unknowns $c(J)$ is

$$n = (r_1+1)\cdots(r_m+1) \sim r_1 r_2 \cdots r_m.$$

Let k be the number of conditions (i.e., the number of I's with $\frac{I}{R} \in \mathfrak{S}(t)$). For large R, we have

$$k \sim r_1 r_2 \cdots r_m W(t).$$

This can be seen in the case $m = 2$ by considering the following picture.



So we have

$$n - dk \sim r_1 r_2 \cdots r_m (1 - dW(t)).$$

Therefore,

$$\frac{dR}{n-dk} < \frac{dW(t)}{1-dW(t)}(1+\epsilon)$$

for R sufficiently large. By Siegel's Lemma 9A of Chapter I, there is a solution of bounded size. More precisely, there exists a polynomial $P \neq 0$ satisfying the index condition, of size

$$\overline{|P|} \leqq ((4h(\alpha_1))^{r_1} \cdots (4h(\alpha_m))^{r_m})^{\frac{dW(t)}{1-w(t)}(1+\epsilon)}.$$

§4. Upper Bounds for the Index.

THEOREM 4A. (Roth's Lemma (1955).) *Suppose $0 < \varepsilon < 1/12$. Put*

$$w = w(m, \varepsilon) = 24 \cdot 2^{-m}(\varepsilon/12)^{2^{m-1}}$$

where $m \in \mathbb{N}$. Let $R = (r_1, \dots, r_m)$ with

$$wr_h \geqq r_{h+1} \qquad (h = 1, \dots, m-1).$$

Suppose $\frac{x_1}{y_1}, \dots, \frac{x_m}{y_m}$ are rationals in reduced form with denominators satisfying

$$y_h^w \geqq 2^{3m} \qquad (h = 1, \dots, m)$$

and

$$y_h^{r_h} \geqq y_1^{r_1} \qquad (h = 1, \dots, m).$$

Let $P(X_1, \dots, X_m) \in \mathbb{Z}[X_1, \dots X_m]$ be such that $P \neq 0$ and

$$\overline{|P|} \leqq y_1^{wr_1}.$$

Suppose P is of multidegree $\leqq R$. Then the index of P at $\left(\frac{x_1}{y_1}, \dots, \frac{x_m}{y_m}\right)$ with respect to R is at most ε.

See Roth (1955), Cassels (1957), or Schmidt (1980) for a proof. Roth's Theorem may be proved either by using Roth's Lemma or Theorem 4B below. Neither of these will be proved in these Notes.

The proof is by induction on m. Here we will only consider the (trivial) case $m = 1$. Let $P(X) \in \mathbb{Z}[X]$ and $\frac{x_1}{y_1}$ a rational with $gcd(x_1, y_1) = 1$. We may write

$$P(X) = \left(X - \frac{x_1}{y_1}\right)^{\ell} M(X)$$

where $M\left(\frac{x_1}{y_1}\right) \neq 0$ and ℓ is the order of vanishing of P at $\frac{x_1}{y_1}$. We can also write

$$P(X) = (y_1 X - x_1)^{\ell} Q(X)$$

where $Q\left(\frac{x_1}{y_1}\right) \neq 0$. Since $P(X) \in \mathbb{Z}[X]$ and $(y_1 X - x_1)$ has integer coefficients and content 1, we get $Q(X) \in \mathbb{Z}[X]$ by Gauss' Lemma. Thus the leading coefficient of P is divisible by y_1^{ℓ} and

$$y_1^{\ell} \leqq \overline{|P|} \leqq y_1^{wr_1} = y_1^{\varepsilon r_1}.$$

Therefore,

$$\frac{\ell}{r_1} \leqq \varepsilon$$

and the index of P at $\frac{x_1}{y_1}$ with respect to $R = (r_1)$ is $\leqq \varepsilon$.

Note that this argument, using Gauss' Lemma, is arithmetical.

Now suppose $P(X_1, \dots, X_m) \in \mathbb{Z}[X_1, \dots X_m]$ is a polynomial of multidegree $\leqq R = (r_1, \dots, r_m)$. The number of coefficients of P is $(r_1 + 1) \cdots (r_m + 1) \sim r_1 r_2 \cdots r_m$ if each r_i is large. Suppose the index of P at $(\alpha_1, \dots, \alpha_m) \in \mathbb{C}^m$ with respect to E is $\geqq t$. Thus $P^I(\alpha_1, \dots, \alpha_m) = 0$ for every I with $\frac{I}{R} \in \mathfrak{S}\left(t, \frac{R}{E}\right)$. The number of such conditions is given asymptotically by $r_1 r_2 \cdots r_m W\left(t, \frac{R}{E}\right)$. Suppose $\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_k \in \mathbb{C}^m$ and the index of P at $\underline{\underline{\alpha}}_h$ with respect to E is $\geqq t_h$ $(h = 1, \dots, k)$. Then the total number of conditions is approximately

$$r_1 r_2 \cdots r_m \sum_{h=1}^{k} W\left(t_h, \frac{R}{E}\right).$$

If these conditions are independent and $P \neq 0$, then $\sum_{h=1}^{k} W\left(t_h, \frac{R}{E}\right)$ should not be much larger than 1.

THEOREM 4B. (Esnault and Viehweg (1984).) *Suppose* $r_1 \geqq r_2 \geqq \cdots \geqq r_m$, *and let* $\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_k \in \mathbb{C}^m$ *with the condition that if* $\underline{\underline{\alpha}}_i = (\alpha_{i1}, \dots, \alpha_{im})$, *then*

$$\alpha_{i\ell} \neq \alpha_{j\ell} \quad \textit{if} \quad i \neq j \qquad (1 \leqq \ell \leqq m).$$

Suppose $P(X_1, \dots, X_m) \in \mathbb{C}(X_1, \dots X_m)$ *of multidegree* $\leqq R$ *with* $P \neq 0$, *and the index of* P *at* $\underline{\underline{\alpha}}_h$ *with respect to* $E = (e_1, \dots e_m)$ *is* $\geqq t_h$ $(h = 1, \dots, m)$. *Then*

$$\sum_{h=1}^{k} W\left(t_h, \frac{R}{E}\right) \leqq \prod_{j=1}^{m-1} \left(1 + (k' - 2) \sum_{i=j+1}^{m} \frac{r_i}{r_j}\right),$$

where $k' = \max(2, k)$.

Bombieri (1982) did the case $m = 2$ before the general case was done. He called this Dyson's Lemma, in reference to work done by Dyson in 1947. For the $m = 2$ case, the bound is slightly better, namely,

$$\sum_{h=1}^{k} W\left(t_h, \frac{R}{E}\right) \leqq 1 + \left(\frac{k' - 1}{2}\right) \frac{r_2}{r_1}.$$

Viola (1985) gave another argument for the $m = 2$ case. He removed the condition $\alpha_{i1} \neq \alpha_{j1}$, $\alpha_{i2} \neq \alpha_{j2}$ for $i \neq j$ and imposed the condition that $P(X_1, X_2)$ have no factor of the form $X_1 - c$ or $X_2 - c$.

Theorem 4B is algebraic in nature. The proof involves a lot of algebraic geometry and will not be given here.

Now suppose K is a number field of degree d. Let $\underline{\underline{\alpha}} = (\alpha_1, \dots, \alpha_m) \in K^m$ with $\mathbb{Q}(\alpha_i) = K$ $(i = 1, \dots, m)$ and $\underline{\underline{\beta}} = (\beta_1, \dots, \beta_m) \in \mathbb{Q}^m$. We will apply Theorem 4B of Esnault and Viehweg with $k = d + 1$ and $\underline{\underline{\alpha}}^{(1)}, \dots, \underline{\underline{\alpha}}^{(d)}, \underline{\underline{\beta}}$. The ℓth coordinates are $\alpha_\ell^{(1)}, \dots, \alpha_\ell^{(d)}, \beta_\ell$, which are all distinct. We will set $t_1 = \cdots = t_d = t$ and $t_{d+1} = \tau$.

If $P(X_1, \dots, X_m) \neq 0$ of multidegree $R = (r_1, \dots, r_m)$ has index $\geqq t$ at $\underline{\underline{\alpha}}^{(i)}$ $(i = 1, \dots, d)$ and index $\geqq \tau$ at $\underline{\underline{\beta}}$ with respect to R, then Theorem 4B gives

$$dW(t) + W(\tau) \leqq \prod_{j=1}^{m-1} \left(1 + (d-1) \sum_{i=j+1}^{m} \frac{r_i}{r_j} \right).$$

Suppose now that

$$\frac{r_{i+1}}{r_i} \leqq \frac{1}{2dm\lambda} \qquad (1 \leqq i \leqq m-1)$$

where $\lambda \geqq 1$. Then (since $d \geqq 2$)

$$\begin{aligned} \sum_{i=j+1}^{m} \frac{r_i}{r_j} &< \frac{1}{2dm\lambda} + \left(\frac{1}{2dm\lambda}\right)^2 + \cdots \\ &< \frac{2}{3dm\lambda}, \end{aligned}$$

and we have

$$\begin{aligned} \prod_{j=1}^{m-1} \left(1 + (d-1) \sum_{i=j+1}^{m-1} \frac{r_i}{r_j} \right) &< \prod_{j=1}^{m-1} \left(1 + \frac{2}{3m\lambda} \right) \\ &< \left(1 + \frac{2}{3m\lambda} \right)^m \\ &< e^{2/3\lambda} < 1 + \frac{1}{\lambda} \end{aligned}$$

since $\lambda \geqq 1$. We have proven the following lemma.

LEMMA 4C. *Suppose $P(X_1, \dots, X_m) \neq 0$ has coefficients in $\mathbb{Q}$ and has multidegree $\leqq R = (r_1, \dots, r_m)$. Furthermore, suppose*

$$\frac{r_{i+1}}{r_i} \leqq \frac{1}{2dm\lambda} \qquad (1 \leqq i \leqq m-1) \tag{4.1}$$

is satisfied with $\lambda \geqq 1$. Suppose $\underline{\underline{\alpha}}$, $\underline{\underline{\beta}}$ are as above and t, τ satisfy

$$dW(t) + W(\tau) \geqq 1 + \frac{1}{\lambda}.$$

Then if P has index $\geqq t$ at $\underline{\underline{\alpha}}$ with respect to R, it follows that P must have index $< \tau$ at $\underline{\underline{\beta}}$ with respect to R.

Exercise 4a. Define $r = r(k,t)$ to be the least integer such that given any k points $\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_k$ in $\mathbb{C}^2$, there exists a polynomial $P(X,Y) \neq 0$ with coefficients in $\mathbb{C}$, of total degree $\leqq r$, and vanishing of order $\geqq t$ at each of $\underline{\underline{\alpha}}_1, \dots \underline{\underline{\alpha}}_k$. Certainly, $r \leqq r_0(k,t)$ where r_0 is least with

$$k\binom{t+1}{2} < \binom{r_0+2}{2}.$$

Thus

$$\overline{\lim}_{t\to\infty}\frac{r(k,t)}{t} \leqq \sqrt{k}\,.$$

Compute the following:

$$r(2,t) \quad \text{and} \quad \lim_{t\to\infty}\frac{r(2,t)}{t},$$

as well as

$$r(3,t) \quad \text{and} \quad \lim_{t\to\infty}\frac{r(3,t)}{t}\,.$$

Exercise 4b. Compute $r(4,t)$ and $r(5,t)$.

§5. Estimation of Volumes.

Recall from §3 that $W(t)$ represents the volume of the set of $(\xi_1,\dots,\xi_m)$ satisfying

$$0 \leqq \xi_i \leqq 1 \qquad (i = 1,\dots,m)$$

and

$$\xi_1 + \cdots + \xi_m \leqq t.$$

LEMMA 5A. *If $t \leqq 1$, then $W(t) = t^m/m!$.*

Remark. If $t \leqq 1$, then $\mathfrak{S}(t)$ is the set of $(\xi_1,\dots,\xi_m)$ satisfying

$$0 \leqq \xi_i \quad \text{and} \quad \xi_1 + \cdots + \xi_m \leqq t.$$

The lemma may be obtained by induction on m.

LEMMA 5B. *If $t = \frac{m}{2} - \theta$ w;here $0 < \theta < \frac{m}{2}$, then $W(t) < e^{-\theta^2/m}$.*

Remark. Consider the cube C consisting of points $(\xi_1,\dots,\xi_m)$ with $0 \leqq \xi_i \leqq 1$ $(i = 1,\dots,m)$. Lemma 5B says that those points satisfying

$$\xi_1 + \cdots + \xi_m \leqq \frac{m}{2} - \theta$$

form a small proportion of C and similarly, by symmetry about $(\frac{1}{2},\dots,\frac{1}{2})$, for those points satisfying

$$\xi_1 + \cdots + \xi_m \geqq \frac{m}{2} + \theta.$$

Thus most points satisfy

$$\left|\xi_1 + \cdots + \xi_m - \frac{m}{2}\right| \leqq \theta,$$

which agrees with probability.

Proof. Set $q = 3\theta/2m$, so that $q \leqq 3/4$. For points in $\mathfrak{S}(t)$, we have

$$\xi_1 + \cdots + \xi_m - \frac{m}{2} \leqq -\theta.$$

Then

$$-q\left(\xi_1 + \cdots + \xi_m - \frac{m}{2}\right) \geqq \theta q = 3\theta^2/2m.$$

Consider

$$\begin{aligned} W(t)e^{3\theta^2/2m} &\leqq \int_0^1 \cdots \int_0^1 \exp\left(-q\left(\xi_1 + \cdots + \xi_m - \frac{m}{2}\right)\right) d\xi_1 \cdots d\xi_m \\ &= \left(\int_0^1 \exp\left(-q\left(\xi - \frac{1}{2}\right)\right) d\xi\right)^m \\ &= I^m, \end{aligned}$$

where I is the integral on the right-hand side. By a change of variables, we get

$$\begin{aligned} I &= \int_{-1/2}^{1/2} \exp(-q\xi) d\xi \\ &= \frac{e^{q/2} - e^{-q/2}}{2} \\ &= \frac{2}{q} \sinh\left(\frac{q}{2}\right) \\ &= \frac{2}{q}\left((q/2) + \frac{1}{3!}(q/2)^3 + \cdots\right) \\ &= 1 + \frac{q^2}{24} + \frac{q^4}{120 \cdot 2^4} + \cdots \\ &< 1 + \frac{q^2}{10} \\ &< e^{q^2/10} = e^{9\theta^2/40m^2} \\ &< e^{\theta^2/4m^2}. \end{aligned}$$

Then

$$W(t)e^{3\theta^2/2m} < e^{\theta^2/4m}$$

and

$$W(t) < e^{-5\theta^2/4m} < e^{-\theta^2/m}.$$

§6. A version of Roth's Theorem.

Let α be algebraic of degree d and $\beta = \frac{x}{y}$. We will consider inequalities of the type

$$|\alpha - \beta| < 1/h(\beta)^{2+\delta}.$$

Given $C > 1$, a *window of exponential width C* will mean an interval of real numbers ξ of type

$$w \leqq \xi < w^C$$

where $w > 1$.

THEOREM 6A. *Suppose α is algebraic of degree $d \geqq 3$. Suppose $1 < m! \leqq d$ and $0 < \chi < 1$. Set $\lambda = 2d(6/\chi)^m$ and $c_m = m/(m!)^{1/m}$. Then the rational solutions β of the inequality*

$$|\alpha - \beta| < h(\beta)^{-c_m d^{1/m}(1+\chi)} \tag{6.1P}$$

have their heights in the union of the interval

$$h(\beta) < (8h(\alpha))^{6\lambda/\chi} = B_1,$$

say, and at most $m - 1$ windows of exponential width C where

$$C = 6dm\lambda = 12d^2m(6/\chi)^m.$$

Remarks. In the case $m = 2$, we get $c_m d^{1/m} = \sqrt{2d}$. Thus if $\sqrt{2d} < \mu < 2\sqrt{2d}$, there is a χ with $\mu = c_m d^{1/m}(1 + \chi)$ and $0 < \chi < 1$. This implies the Dyson–Gelfond estimate. In this case, we have at most 1 window.

In the case $m = 3$, we get $c_m = 3/\sqrt[3]{6} = \sqrt[3]{9/2}$ and $\mu > \sqrt[3]{9/2} \cdot \sqrt[3]{d}$. In this case, there are two possible windows.

THEOREM 6B. *Suppose α is algebraic of degree $d \geqq 3$. Suppose $0 < \delta < 1$ and $m = [(25/\delta)^2 \log 2d]$. Let $\lambda = 2m!$. Then the rational solutions β of the inequality*

$$|\alpha - \beta| < h(\beta)^{-2-\delta}$$

have their heights in the union of the interval

$$h(\beta) < (4h(\alpha))^{25\lambda/\delta} = B_2,$$

say, and at most $m - 1$ windows of exponential width $C = 6dm\lambda$.

Remark. Theorem 6B contains Roth's Theorem.

Let α be given in a number field K with $\deg K = d$ and $K = \mathbb{Q}(\alpha)$. Furthermore, let $\beta \in \mathbb{Q}$ and $\lambda > 1$ be given. We introduce the *mixed height* of α and β, given by

$$h_\lambda(\alpha, \beta) = (4h(\alpha))^\lambda \cdot 4h(\beta).$$

We will now state the main theorems.

THEOREM 6C. *Let $(\alpha_1, \beta_1), \dots, (\alpha_m, \beta_m)$ be such that $\mathbb{Q}(\alpha_i) = K$ and $\beta_i \in \mathbb{Q}$ $(i = 1, \dots, m)$. Suppose that*

(i) $1 < m! \leqq d$,

(ii) $\lambda \geqq 2d \cdot 4^m$,

(iii) $|\alpha_i - \beta_i| < h_\lambda(\alpha_i, \beta_i)^{-c_m d^{1/m}(1+4(2d/\lambda)^{1/m})}$ $(i = 1, \dots, m)$,

(iv) $h_\lambda(\alpha_{i+1},\beta_{i+1}) > h_\lambda(\alpha_i,\beta_i)^{3dm\lambda}$ $(i = 1,\dots,m-1)$.
This is impossible!

THEOREM 6D. *Let* $(\alpha_1,\beta_1),\dots,(\alpha_m,\beta_m)$ *be as above, and suppose that*
(i) $m > 36\log 2d$,
(ii) $\lambda \geqq 2m!$,
(iii) $|\alpha_i - \beta_i| < h_\lambda(\alpha_i,\beta_i)^{-2-12\sqrt{(\log 2d)/m}}$ $(i = 1,\dots,m)$,
(iv) *as above.*
This is impossible.

Remark. Theorems 6C and 6D give Theorems 6A and 6B, respectively.

First, we will verify that Theorem 6C implies Theorem 6A. Consider solutions β of (6.1), i.e.

$$|\alpha - \beta| < h(\beta)^{c_m d^{1/m}(1+\chi)}.$$

Let $B_1 = (8h(\alpha))^{6\lambda/\chi}$, and suppose $h(\beta) \geqq B_1$. Let $\lambda = 2d(6/\chi)^m$. Then $\chi = 6(2d/\lambda)^{1/m}$ and (6.1) implies that

$$\begin{aligned}|\alpha - \beta| &< h(\beta)^{-c_m d^{1/m}(1+\frac{2}{3}\chi)} h(\beta)^{-c_m d^{1/m}(\frac{1}{3}\chi)}\\ &< h(\beta)^{-c_m d^{1/m}(1+4(2d/\lambda)^{1/m})}(8h(\alpha))^{-c_m d^{1/m}\cdot 2\lambda}\\ &< h_\lambda(\alpha,\beta)^{-c_m d^{1/m}(1+4(2d/\lambda)^{1/m})},\end{aligned}$$

since $2 > 1+4(2d/\lambda)^{1/m}$ and $8^\lambda > (4^\lambda)\cdot 4$. If there is no approximation β with $h(\beta) \geqq B_1$, then we are finished. Otherwise, let β_1 have minimal height with $h(\beta) \geqq B_1$. If each such β has $h(\beta) < h(\beta_1)^{6dm\lambda}$, then they all lie in a single window and we are done. Otherwise, let β_2 have minimal height with $h(\beta) \geqq h(\beta_1)^{6dm\lambda}$. Then

$$\begin{aligned}h_\lambda(\alpha,\beta_2) > h(\beta_2) &\geqq h(\beta_1)^{3dm\lambda}\cdot B_1^{3dm\lambda}\\ &\geqq (h(\beta_1)\cdot(8h(\alpha))^\lambda)^{3dm\lambda}\\ &\geqq h_\lambda(\alpha_1,\beta_1)^{3dm\lambda}.\end{aligned}$$

Continue in this fashion. If the solutions with $h(\beta) \geqq B_1$ do not lie in $m-1$ windows, then $\beta_1,\beta_2,\dots,\beta_m$ can be found, and Theorem 6C with $\alpha_i = \alpha$ $(i = 1,\dots,m)$ gives a contradiction.

Next, we will show that Theorem 6D implies Theorem 6B. Suppose that $|\alpha - \beta| < h(\beta)^{-2-\delta}$ and

$$h(\beta) \geqq B_2 = (4h(\alpha))^{25\lambda/\delta}.$$

With m, λ as in Theorem 6B, we have

$$\frac{\log 2d}{m} < \left(\frac{\delta}{24}\right)^2, \qquad \sqrt{(\log 2d)/m} > \frac{\delta}{24}.$$

We infer that

$$\begin{aligned}|\alpha-\beta| &< h(\beta)^{-2-\delta/2}h(\beta)^{-\delta/2}\\ &< h(\beta)^{-2-12\sqrt{(\log 2d)/m}}\,B_2^{-12\sqrt{(\log 2d)/m}}\\ &< h(\beta)^{-2-12\sqrt{(\log 2d)/m}}\,(4h(\alpha))^{-300\lambda\sqrt{(\log 2d)/m}}/\delta.\end{aligned}$$

But since

$$\frac{\log 2d}{m} \geqq \left(\frac{\delta}{25}\right)^2, \qquad \sqrt{(\log 2d)/m}\,/\delta > \frac{1}{25},$$

we obtain

$$\begin{aligned}|\alpha-\beta| &< h(\beta)^{-2-12\sqrt{(\log 2d)/m}}\,(4h(\alpha))^{-12\lambda}\\ &< h_\lambda(\alpha,\beta)^{-2-12\sqrt{(\log 2d)/m}}.\end{aligned}$$

We now proceed as with Theorem 6A: If there is no approximation β with $h(\beta) \geqq B_2$, then we are finished. Otherwise, ...

§7. Proof of the Main Theorems, i.e., Theorems 6C, 6D.

Suppose $(\alpha_1,\beta_1),\dots,(\alpha_m,\beta_m)$ are given such that $\mathbb{Q}(\alpha_i) = K$ and $\beta_i \in \mathbb{Q}$ $(i = 1,\dots,m)$. Pick $t = t(m,\lambda)$ such that $dW(t) = 1-(1/\lambda)$, and τ such that $W(\tau) = 2/\lambda$. We will use Lemma 3A to construct a polynomial $P(X_1,\dots,X_m)$ of multidegree $R = (r_1,\dots,r_m)$, where the r_i are large, such that P has index $\geqq t$ at $(\alpha_1,\dots,\alpha_m)$ with respect to R. We can choose $r_1,\dots,r_m$ such that

$$\frac{r_{i+1}}{r_i} \leqq \frac{1}{2dm\lambda} \qquad (i = 1,\dots,m-1).$$

Then by Lemma 4C, we know that P will have index $< \tau$ at $(\beta_1,\dots,\beta_m) \in \mathbb{Q}$. Thus there exists an $I = (i_1,\dots,i_m)$ with

$$\frac{i_1}{r_1}+\dots+\frac{i_m}{r_m} < \tau \tag{7.1}$$

such that $P^I(\underline{\beta}) \neq 0$. Set $Q(\mathbf{X}) = P^I(\mathbf{X})$. Then by (3.1) we have $|\overline{P^I}| = |\overline{Q}| \leqq 2^r|\overline{P}|$ where $r = r_1+\dots+r_m$. Moreover, by (3.2) we have $|\overline{Q^J}| \leqq 3^r|\overline{P}|$ for any J. Since P had index $\geqq t$ at $\underline{\alpha}$, it follows from (7.1) that $Q = P^I$ has index $\geqq t-\tau$ at $\underline{\alpha}$ (with respect to R). Since

$$\frac{dW(t)}{1-dW(t)} = \frac{1-(1/\lambda)}{(1/\lambda)} = \lambda - 1,$$

we have

$$\frac{dW(t)}{1-dW(t)}(1+\varepsilon) < \lambda$$

for $\varepsilon > 0$ sufficiently small. Then by Lemma 3A, the polynomial P can be constructed such that

$$|\overline{P}| \leqq ((4h(\alpha_1))^{r_1}\cdots(4h(\alpha_m))^{r_m})^\lambda.$$

Then

$$|\overline{Q^J}| \leqq 3^r|\overline{P}| \leqq 3^r((4h(\alpha_1))^{r_1}\cdots(4h(\alpha_m))^{r_m})^{\lambda}.$$

Writing $\beta_i = x_i/y_i$ $(i = 1,\dots,m)$, we have $y_1^{r_1}\cdots y_m^{r_m}Q(\underline{\underline{\beta}}) \in \mathbb{Z}\backslash\{0\}$. Thus

$$\left|y_1^{r_1}\cdots y_m^{r_m}Q(\underline{\underline{\beta}})\right| \geqq 1.$$

Writing the Taylor's expansion for Q about $\underline{\underline{\alpha}}$ gives

$$Q(\underline{\underline{\beta}}) = \sum_{\substack{J=(j_1,\dots,j_m)\\ \frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m} \geqq t-\tau}} (\beta_1-\alpha_1)^{j_1}\cdots(\beta_m-\alpha_m)^{j_m}Q^J(\underline{\underline{\alpha}})$$

where the sum is restricted to $\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m} \geqq t-\tau$ since all lower order partial derivatives vanish at $\underline{\underline{\alpha}}$. By condition (iii), we have

$$|\alpha_i-\beta_i| < 1/2 \qquad (i=1,\dots,m),$$

which gives

$$|\alpha_i| < |\beta_i| + \frac{1}{2} = \left|\frac{x_i}{y_i}\right| + \frac{1}{2} = \frac{|x_i|+(1/2)|y_i|}{y_i} \quad (i=1,\dots,m).$$

Applying Cauchy's inequality to the right-hand side gives

$$|\alpha_i| \leqq \frac{\sqrt{5/4}\,h(\beta_i)}{y_i} \qquad (i=1,\dots,m).$$

Now we have

$$|Q^J(\underline{\underline{\alpha}})| \leqq |\overline{Q^J}|\left(\prod_{i=1}^{m}(r_i+1)\right)\left(\frac{\sqrt{5/4}\,h(\beta_1)}{y_i}\right)^{r_1}\cdots\left(\frac{\sqrt{5/4}\,h(\beta_m)}{y_m}\right)^{r_m},$$

and therefore

$$\left|y_1^{r_1}\cdots y_m^{r_m}Q^J(\underline{\underline{\alpha}})\right| \leqq 3^r|\overline{P}|\left(\prod_{i=1}^{m}(r_i+1)\right)\left(\prod_{i=1}^{m}\left(\sqrt{\frac{5}{4}}\,h(\beta_i)\right)^{r_i}\right).$$

The Taylor expansion for Q gives us

$$\begin{aligned}
&\left|y_1^{r_1}\cdots y_m^{r_m}Q(\underline{\underline{\beta}})\right| \\
&\leqq 3^r|\overline{P}|\left(\prod_{i=1}^{m}(r_i+1)^2\right)\left(\prod_{i=1}^{m}\left(\sqrt{\frac{5}{4}}\,h(\beta_i)\right)^{r_i}\right)\max_{\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\geqq t-\tau}(|\beta_1-\alpha_1|^{j_1}\cdots|\beta_m \\
&\qquad -\alpha_m|^{j_m}) \\
&=|\overline{P}|\left(\prod_{i=1}^{m}(r_i+1)^2\right)\left(\prod_{i=1}^{m}\left(3\sqrt{\frac{5}{4}}\,h(\beta_i)\right)^{r_i}\right)\max_{\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\geqq t-\tau}(|\alpha_1-\beta_1|^{j_1}\cdots|\alpha_m \\
&\qquad -\beta_m|^{j_m}).
\end{aligned}$$

So for r_i large,

$$\left|y_1^{r_1}\cdots y_m^{r_m}Q(\underline{\underline{\beta}})\right|<\left(\prod_{i=1}^{m}(4h(\beta_i))^{r_i}\right)|\overline{P}|\max_{\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\geqq t-\tau}(|\alpha_1-\beta_1|^{j_1}\cdots|\alpha_m-\beta_m|^{r_m}),$$

and

$$1\leqq\left(\prod_{i=1}^{m}(h_\lambda(\alpha_i,\beta_i))^{r_i}\right)\max_{\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\geqq t-\tau}(|\beta_1-\alpha_1|^{r_1}\cdots|\beta_m-\alpha_m|^{r_m}). \qquad (7.2)$$

Now suppose that

$$|\beta_i-\alpha_i|\leqq h_\lambda(\alpha_i,\beta_i)^{-\psi}$$

with $\psi>0$. Then (7.2) yields

$$1\leqq\left(\prod_{i=1}^{m}(h_\lambda(\alpha_i,\beta_i))^{r_i}\right)\max_{\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\geqq t-\tau}(h_\lambda(\alpha_1,\beta_1)^{-j_1\psi}\cdots h_\lambda(\alpha_m,\beta_m)^{-j_m\psi}).$$

Following Bombieri and Van der Poorten (1987) we take logarithms of both sides. Write $L_i=\log h_\lambda(\alpha_i,\beta_i)$, $(i=1,\ldots,m)$. We then obtain

$$0\leqq r_1L_1+\cdots+r_mL_m-\psi\min_{\frac{j_1}{r_1}+\cdots+\frac{j_m}{r_m}\geqq t-\tau}(j_1L_1+\cdots+j_mL_m).$$

Putting $\varphi_i=j_i/r_i$ $(i=1,\ldots,m)$, we have

$$((7.3))\qquad r_1L_1+\cdots r_mL_m\geqq\psi\min_{\substack{\varphi_1+\cdots+\varphi_m\geqq t-\tau\\ \varphi_i\in\mathbb{R}}}(\varphi_1r_1L_1+\cdots\varphi_mr_mL_m).$$

Now choose $r_i=[L/L_i]$ $(i=1,\ldots,m)$ where L is large. By condition (iv), we have $L_{i+1}>3dm\lambda L_i$ $(i=1,\ldots,m-1)$, so that

$$\frac{r_{i+1}}{r_i}<\frac{1}{2dm\lambda}\qquad(i=1,\ldots,m-1).$$

Dividing (7.3) by L and letting $L \to \infty$, we get

$$m \geqq \psi \min_{\substack{\varphi_1+\cdots+\varphi_m \geqq t-\tau \\ \varphi_i \in \mathbb{R}}} (\varphi_1 + \cdots + \varphi_m) = \psi(t-\tau).$$

Hence

$$\psi \leqq \frac{m}{t-\tau} \tag{7.4}$$

This is the key inequality. Using it together with estimates for m, t, and τ, we will prove the two main theorems.

Recall that $dW(t) = 1 - (1/\lambda)$ and $W(\tau) = 2/\lambda$. In Theorem 6C, we have (i) $1 < m! \leqq d$ and (ii) $\lambda \geqq 2d \cdot 4^m$. This gives

$$W(t) < \frac{1}{d} \leqq \frac{1}{m!}$$

and

$$W(\tau) < \frac{1}{d} \nleqq \frac{1}{m!},$$

so that we can apply Lemma 5A in both cases. That is,

$$\begin{aligned} W(t) &= \frac{t^m}{m!}, \\ d\frac{t^m}{m!} &= \left(1 - \frac{1}{\lambda}\right), \\ t &= (m!)^{1/m} \left(\frac{1}{d}\left(1 - \frac{1}{\lambda}\right)\right)^{1/m}, \end{aligned}$$

and

$$\begin{aligned} W(\tau) &= \frac{\tau^m}{m!}, \\ \frac{2}{\lambda} &= \frac{\tau^m}{m!}, \\ \tau &= (m!)^{1/m}(2/\lambda)^{1/m}. \end{aligned}$$

So we have

$$\begin{aligned} t - \tau &= (m!)^{1/m} d^{-1/m} \left(\left(1 - \frac{1}{\lambda}\right)^{1/m} - (2d/\lambda)^{1/m}\right) \\ &\geqq (m!)^{1/m} d^{-1/m} \left(\left(1 - \frac{1}{\lambda}\right) - (2d/\lambda)^{1/m}\right) \\ &= (m!)^{1/m} d^{-1/m} (1 - \eta) \end{aligned}$$

where

$$\begin{aligned} \eta &= (1/\lambda) + (2d/\lambda)^{1/m} \\ &\leqq 2(2d/\lambda)^{1/m} \\ &\leqq 1/2 \qquad \text{(by (ii))}. \end{aligned} \tag{7.5}$$

Observe that

$$\frac{1}{1-\eta} \leqq 1+2\eta \leqq 1+4(2d/\lambda)^{1/m} \quad \text{(by (7.5))}.$$

Therefore

$$t-\tau \geqq (m!)^{1/m} d^{-1/m}(1+4(2d/\lambda)^{1/m})^{-1}.$$

Now we are in a position to estimate ψ with

$$|\beta_i-\alpha_i| \leqq h_\lambda(\alpha_i,\beta_i)^{-\psi}.$$

By (7.4) we have

$$\begin{aligned}\psi &\leqq \frac{m}{t-\tau}\\ &\leqq \frac{m}{(m!)^{1/m}} d^{1/m}(1+4(2d/\lambda)^{1/m})\\ &= c_m d^{1/m}(1+4(2d/\lambda)^{1/m}).\end{aligned}$$

However, in Theorem 6C (iii), we have

$$|\alpha_i-\beta_i| < h_\lambda(\alpha_i,\beta_i)^{-c_m d^{1/m}(1+\overset{(2}{4d}/\lambda)^{1/m})},$$

which gives a contradiction.

We now turn to Theorem 6D. As before, $dW(t) = 1-(1/\lambda)$ and $W(\tau) = 2/\lambda \leqq 1/(m!)$ by (ii). Since $W(\tau)$ is an increasing function of τ, we may infer from Lemma 5A that $\tau \leqq 1$. Next, $d \geqq 2$ gives us $W(t) < 1/2$. Therefore $t < m/2$, say $t = (m/2)-\theta$ with $0 < \theta < m/2$. Then by Lemma 5B,

$$W(t) < e^{-\theta^2/m},$$

so that

$$\frac{1}{d}\left(1-\frac{1}{\lambda}\right) < e^{-\theta^2/m}.$$

Now we have

$$\begin{aligned}e^{\theta^2/m} &< d\left(1-\frac{1}{\lambda}\right)^{-1}\\ &\leqq 2d \qquad \text{(by (ii))}.\end{aligned}$$

Taking the logarithm of both sides gives

$$\theta < \sqrt{m\log 2d}$$

and

$$t > (m/2)-\sqrt{m\log 2d}.$$

So

$$t-\tau > (m/2)-1-\sqrt{m\log 2d}.$$

Now we may return to our task of estimating ψ. By (7.4),

$$\psi \leqq \frac{m}{t-\tau},$$

so that we obtain

$$\begin{aligned}\psi &\leqq \frac{m}{(m/2) - 1 - \sqrt{m \log 2d}} \\ &= \frac{2}{1 - (2/m) - 2\sqrt{(\log 2d)/m}} \\ &< \frac{2}{1 - 3\sqrt{(\log 2d)/m}} \\ &< 2(1 + 6\sqrt{(\log 2d)/m}\,) \quad \text{(by (i))} \\ &= 2 + 12\sqrt{(\log 2d)/m}\,.\end{aligned}$$

But Theorem 6D (iii) is

$$|\alpha_i - \beta_i| < h_\lambda(\alpha_i, \beta_i)^{-2-12\sqrt{(\log 2d)/m}},$$

which gives the desired contradiction.

§8. **Counting Good Rational Approximations.** In the summer of 1987, in the course of a number theory conference in Budapest, A. Schinzel asked the following, almost philosophical question: "But how can it be, how can it be in *number theory*, that one could prove the finiteness of a set of natural numbers, without being able to give a bound for its cardinality?" The next day he himself provided the following explanation.

Suppose we are given a set S of positive integers and suppose we can prove that if y, y' are in S, then $y' \leqq 2y$. Then S must be finite. However, unless we know at least one y in S, we are unable to estimate the cardinality of S without further information. We will generalize Schinzel's remark as follows. Given $C > 1$, a set S of positive numbers is a *C–set*, if for any y, y' in S we have $y' \leqq Cy$. Any C–set consisting of integers is finite.

Now let $\gamma > 1$ be given.

A *γ–set* is a set of positive real numbers with the following property: if y, y' are in the set and $y < y'$, then $y' \geqq \gamma y$. Thus a γ–set has a certain "Gap Principle". A set which is both a C–set and a γ–set will be called a *(C, γ)–set.* Its elements are positive real numbers, not necessarily integers.

LEMMA 8A. *Suppose $C > 1$ and $\gamma > 1$ are given. The cardinality of any (C, γ)–set is*

$$\leqq 1 + (\log C)/\log \gamma.$$

Proof. Let $C > 1$ and $\gamma > 1$ be given. Suppose $y_0 < y_1 < y_2 < \cdots < y_\nu$ belong to a (C, γ)–set. Then

$$y_i \geqq y_0 \cdot \gamma^i \qquad (i = 0, \ldots, \nu)$$

and

$$Cy_0 \geqq y_\nu \geqq y_0 \gamma^\nu.$$

Therefore

$$\nu \leqq (\log C)/\log \nu,$$

and the cardinality of the (C,γ)-set is

$$\leqq 1+(\log C)/\log\gamma.$$

Suppose $\delta>0$. Let

$$L=\log(1+\delta). \tag{8.1}$$

LEMMA 8B. *Let a real number ξ be given. The number of reduced fractions (x/y) with*

$$\left|\xi-\frac{x}{y}\right|<\frac{1}{2y^{2+\delta}} \tag{8.2}$$

and y in a window of exponential width C is

$$\leqq 1+(\log C)/L.$$

Proof. If y,y' are in a window of exponential width C, then $y'\leqq y^C$. We will call this an *exponential C-set.* Now, if $x/y, x'/y'$ satisfy the hypotheses and $x/y\neq x'/y'$, say $y'\geqq y$, then

$$\begin{aligned}\frac{1}{yy'} &\leqq \left|\frac{x}{y}-\frac{x'}{y'}\right|\\ &\leqq \left|\xi-\frac{x}{y}\right|+\left|\xi-\frac{x'}{y'}\right|\\ &< \frac{1}{2y^{2+\delta}}+\frac{1}{2y'^{2+\delta}}\\ &\leqq \frac{1}{y^{2+\delta}},\end{aligned}$$

and we have

$$y'>y^{1+\delta}=y^{\gamma},$$

where $\gamma=1+\delta$. We call such a set an *exponential γ-set.* The logarithms of the numbers y form a (C,γ)-set. By Lemma 8A its cardinality is

$$\leqq 1+\frac{\log C}{\log\gamma}=1+\frac{\log C}{L}.$$

Suppose now that $1<A<B$ are given, and consider rational approximations to ξ with

$$\left|\xi-\frac{x}{y}\right|<\frac{1}{2y^{2+\delta}}$$

and $A\leqq y\leqq B$. The denominators y lie in a window of exponential width $C=(\log B)/\log A$. Therefore, Lemma 8B says the number of such y is

$$\leqq 1+\frac{\log(\log B/\log A)}{L}.$$

There are a couple of drawbacks to Lemma 8B. We cannot let A go to 1, since $C = (\log B)/\log A$. Secondly, we have a 2 in the denominator in (8.2). We will try to remove these drawbacks. For $\delta > 0$, we will call x/y a *δ–approximation* to ξ if $y > 0$ and $(x, y) = 1$ and

$$\left|\xi - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}}. \tag{8.3}$$

Then we have the following results.

LEMMA 8C. *The number of δ–approximations to ξ with y in a window $W \leqq y \leqq W^C$ where $W \geqq 4^{1/\delta}$ is*

$$\leqq 1 + (\log 2C)/L.$$

Proof. Suppose x/y and x'/y' are such approximations and $y' \geqq y$. Using the same argument as above (i.e., in the proof of Lemma 8B), we get

$$y' \geqq y^{1+\delta}/2.$$

Then

$$\log y' \geqq (1 + \delta)\log y - \log 2.$$

Now suppose that x_0/y_0, $x_1/y_1, \ldots, x_\nu/y_\nu$ are such approximations with $y_0 \leqq y_1 \leqq \cdots \leqq y_\nu$. Then

$$\begin{aligned}
\log y_1 &\geqq (1+\delta)\log y_0 - \log 2,\\
\log y_2 &\geqq (1+\delta)\log y_1 - \log 2\\
&\geqq (1+\delta)^2 \log y_0 - ((1+\delta) + 1)\log 2,\\
&\vdots\\
\log y_\nu &\geqq (1+\delta)^\nu \log y_0 - ((1+\delta)^{\nu-1} + \cdots + (1+\delta) + 1)\log 2\\
&\geqq (1+\delta)^\nu(\log W - (\log 2)/\delta).
\end{aligned}$$

Since $W \geqq 4^{1/\delta}$, we have

$$\log W \geqq (\log 4)/\delta = 2(\log 2)/\delta$$

and

$$\log y_\nu \geqq (1+\delta)^\nu(\log W)/2.$$

We also have $y_\nu \leqq W^C$, so that

$$C\log W \geqq \log y_\nu \geqq (1+\delta)^\nu(\log W)/2.$$

Thus

$$(1+\delta)^\nu \leqq 2C$$

and

$$\nu \leqq (\log 2C)/L.$$

The lemma follows.

THEOREM 8D. *The number of δ–approximations with denominators $y \leqq B$, where $B \geqq e$, is*

$$< L^{-1} \log\log B + 20((1/\delta) + 1).$$

Recall, $L = \log(1 + \delta)$, as in (8.1).

Thjs result, as well as Theorem 8E below, is due to Mueller and Schmidt (1989).

Proof. We will say that "large solutions" are those with $e^{2/\delta} \leqq y \leqq B$. These form a window of exponential width

$$C = \frac{\log B}{\log e^{2/\delta}} = \frac{\delta}{2} \log B.$$

By Lemma 8C, the number of solutions here is

$$\begin{aligned} &\leqq 1 + \frac{\log(\delta \log B)}{L} \\ &= \frac{\log\log B}{L} + 1 + \frac{\log \delta}{L} \\ &< \frac{\log\log B}{L} + 2, \end{aligned}$$

since $L = \log(1 + \delta) > \log \delta$.

We will let "small solutions" be those with $y < e^{2/\delta}$. Given an integer u, let the set $S(u)$ consist of δ–approximations with $e^u \leqq y < e^{u+1}$. Suppose $\frac{x_0}{y_0} < \frac{x_1}{y_1} < \cdots < \frac{x_\mu}{y_\mu}$ are elements of $S(u)$. Any two consecutive elements cannot be too close, since

$$\frac{x_{i+1}}{y_{i+1}} - \frac{x_i}{y_i} \geqq \frac{1}{y_i y_{i+1}} > e^{-2u-2} \quad (i = 0, \ldots, \mu - 1).$$

We may conclude that

$$\frac{x_\mu}{y_\mu} - \frac{x_0}{y_0} > \mu e^{-2u-2}.$$

On the other hand, we have

$$\begin{aligned} \frac{x_\mu}{y_\mu} - \frac{x_0}{y_0} &\leqq \left|\xi - \frac{x_0}{y_0}\right| + \left|\xi - \frac{x_\mu}{y_\mu}\right| \\ &< \frac{1}{y_0^{2+\delta}} + \frac{1}{y_\mu^{2+\delta}} \\ &\leqq 2e^{-u(2+\delta)}. \end{aligned}$$

Combining these two estimates, we get $\mu < 2e^{2-u\delta}$, and hence

$$\operatorname{card}(S(u)) = 1 + \mu < 1 + 2e^{2-u\delta}.$$

The "small approximations" lie in the union of $S(0), S(1), \ldots, S(k)$ where $k = [\log e^{2/\delta}] < 2/\delta$. So the total number of "small" δ-approximations is

$$
\begin{aligned}
&\leqq \sum_{u=0}^{k} (1 + 2e^{2-u\delta}) \\
&< k + 1 + 2e^2 \sum_{u=0}^{\infty} e^{-u\delta} \\
&< \frac{2}{\delta} + 1 + 2e^2(1 - e^{-\delta})^{-1} \\
&\leqq 1 + \frac{2}{\delta} + 2e^2\left(\frac{1}{\delta} + 1\right) \\
&< 17\left(\frac{1}{\delta} + 1\right).
\end{aligned}
$$

Adding the estimates for the numbers of "small" and "large" δ-approximations, we get a bound which is less than

$$L^{-1} \log\log B + 20((1/\delta) + 1).$$

The following theorem tells us that the main term in the conclusion of Theorem 8D (i.e., $L^{-1} \log\log B$) is indeed best possible.

THEOREM 8E. *Let $\delta > 0$ be given. There exists a real transcendental number ξ such that for every $B \geqq e$, the number of δ-approximations with $y \leqq B$ is*

$$\geqq \frac{\log\log B}{L} + \frac{\log(\delta/2)}{L}.$$

The proof uses continued fractions. For an introduction to continued fractions, see Hardy and Wright (1954), or Cassels (1957), or Schmidt (1980).

Proof. Given natural numbers $a_1, \ldots, a_n$, write

$$\cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}} = \frac{p_n}{q_n}$$

with $q_n > 0$ and g.c.d. $(p_n, q_n) = 1$. We will define a sequence $a_1, a_2, \ldots$ inductively. Set $a_1 = 1$. Given $a_1, \ldots, a_n$, let a_{n+1} be the least integer with‡

$$a_{n+1}q_n + q_{n-1} \geqq 2q_n^{1+\delta}.$$

‡The factor 2 on the righthand side is not needed for our present purpose but will come in handy in §9.

Then since (by the theory of continued fractions) $q_{n+1} = a_{n+1}q_n + q_{n-1}$, we have

$$2q_n^{1+\delta} \leqq q_{n+1} \leqq 3q_n^{1+\delta}.$$

Again from the theory of continued fractions, the limit $\lim_{n\to\infty} p_n/q_n$ exists. Denote this limit by ξ. It is customary to write

$$\xi = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

and to interpret the right hand side as an "infinite continued fraction".

It is known that

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}},$$

so that in our case

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^{2+\delta}}. \tag{8.4}$$

We would like to know how fast these denominators grow. We have

$$\begin{aligned} q_1 &= 1, & \log q_1 &= 0, \\ q_2 &\leqq 3q_1^{1+\delta}, & \log q_2 &\leqq \log 3, \\ q_3 &\leqq 3q_2^{1+\delta}, & \log q_3 &\leqq ((1+\delta)+1)\log 3. \end{aligned}$$

For arbitrary n, the inequality is

$$\begin{aligned} \log q_n &\leqq ((1+\delta)^{n-2} + \cdots + (1+\delta) + 1)\log 3 \\ &< \frac{(1+\delta)^{n-1}}{\delta}\log 3. \end{aligned}$$

So the number of $q_n \leqq B$ is at least N, where N is the largest integer with

$$\frac{(1+\delta)^{N-1}}{\delta}\log 3 \leqq \log B.$$

Then

$$(1+\delta)^N > \frac{\delta}{\log 3}\log B$$

and

$$\begin{aligned} N &> L^{-1}\log(\delta \log B/\log 3) \\ &> L^{-1}\log\log B + L^{-1}\log(\delta/2). \end{aligned}$$

Since we have infinitely many δ–approximations, we know that ξ is transcendental by Roth's Theorem.

Exercise 8a. The number of approximations x/y in reduced form with

$$\left|\xi - \frac{x}{y}\right| < \frac{1}{y^2 \log y}$$

and $2 \leqq y \leqq B$ is

$$\leqq (1+\varepsilon)\frac{\log B}{\log\log B}$$

when $B > B_0(\varepsilon)$.

§9. The Number of Good Approximations to Algebraic Numbers.

THEOREM 9A. *Suppose that α is algebraic of degree $d \geqq 3$, that m satisfies $1 < m! < d$, and that $\mu = c_m d^{1/m}(1+\chi)$ where $\chi > 0$. Then the number of approximations x/y to α with*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^\mu} \tag{9.1}$$

is

$$\underset{m,\chi}{\ll} 1 + \frac{\log^+ \log h(\alpha)}{\log d},^*$$

‡
where $\underset{m,\chi}{\ll}$ means that the implicit constant may depend on m and χ. Furthermore, the number of such approximations with $y \geqq h(\alpha)$ is

$$\underset{m,\chi}{\ll} 1.$$

Consider the case $m = 2$. Then, e.g., $\mu = 3\sqrt{d}/2$ has $\mu = \sqrt{2d}(1+\chi)$ for some $\chi > 0$. Theorem 9A says the number of approximations satisfying

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{3\sqrt{d}/2}}$$

‡$\log^+ z = \begin{cases} \log z & \text{if } z > 1, \\ 0 & \text{if } 0 < z \leqq 1 \end{cases}$

is bounded as indicated, i.e.,

$$\ll 1 + \frac{\log^+ \log h(\alpha)}{\log d}.$$

Proof. We may suppose that $0 < \chi < 1$. Then $\mu > c_m d^{1/m} \geqq c_m 3^{1/m} > 2.1$. As before, we distinguish between "small" and "large solutions".

"Small solutions" will be those satisfying

$$y < (8h(\alpha))^{12\lambda/\chi} = B_1,$$

where $\lambda = 2d(12/\chi)^m$. By Theorem 8B with $\delta = \mu - 2$, the number of such approximations is

$$\ll \frac{\log\log B}{\log(\mu-1)} + \frac{1}{\mu-2} + 1$$
$$\ll \frac{\log\log B_1}{\log d} + 1.$$

(Here and in the rest of this section, $\ll$ means $\underset{m,\chi}{\ll}$.)

We will estimate $\log\log B_1$. Since

$$\log B_1 = \frac{12\lambda}{\chi}\log(8h(\alpha))$$
$$= 2d\left(\frac{12}{\chi}\right)^{m+1}\log(8h(\alpha)),$$

we have that

$$\log\log B_1 \ll \log d + \log^+ \log h(\alpha) + 1.$$

Thus the number of "small solutions" is

$$\ll \frac{\log^+ \log h(\alpha)}{\log d} + 1.$$

Now consider the "large solutions", i.e., those satisfying

$$y \geqq (8h(\alpha))^{12\lambda/\chi} = B_1.$$

We will write $\beta = x/y$. We have from (9.1) that

$$\left|\frac{x}{y}\right| < |\alpha| + 1,$$

so that

$$h(\beta) < (|\alpha| + 2)y$$
$$\leqq 3h(\alpha)^d y,$$

since $|\alpha| \leqq h(\alpha)^d$. Now consider

$$\begin{aligned} y^\mu &= y^{c_m d^{1/m}(1+\chi)} \\ &= y^{c_m d^{1/m}(1+(\chi/2))} y^{c_m d^{1/m}(\chi/2)} \\ &\geqq h(\beta)^{c_m d^{1/m}(1+(\chi/2))}((3h(\alpha)^d)^{-2} y^{\chi/2})^{c_m d^{1/m}}. \end{aligned}$$

Since

$$y > (3h(\alpha)^d)^{4/\chi},$$

we have

$$(3h(\alpha)^d)^{-2} y^{\chi/2} > 1,$$

so that

$$y^\mu > h(\beta)^{c_m d^{1/m}(1+(\chi/2))}.$$

We therefore obtain

$$|\alpha - \beta| < h(\beta)^{-c_m d^{1/m}(1-(\chi/2))}.$$

Apply Theorem 6A with $\chi/2$ in place of χ. Then we have either $h(\beta) < B_1$, or $h(\beta)$ lies in the union of at most $m-1$ windows of exponential width $C = 6dm\lambda$ where $\lambda = 2d(12/\chi)^m$. We also know that the first case is ruled out because $h(\beta) \geqq y \geqq B_1$. Therefore, by Lemma 8C, the number of solutions is not greater than

$$1 + \frac{\log 2C}{\log(\mu - 1)}.$$

We know that $2C = 2d^2(12/\chi)^m m$, so that

$$\log 2C \ll 1 + \log d.$$

Also,

$$\log(\mu - 1) \gg \log \mu \gg \log d.$$

So the number of solutions in such windows is $\ll 1$, and the main statement of the theorem is proven.

We have already seen that the number of approximations with $y \geqq B_1$ is $\ll 1$. It remains to count the solutions with y in the interval

$$h(\alpha) \leqq y \leqq B_1.$$

Recall that

$$B_1 = (8h(\alpha))^{12\lambda/\chi}$$

and

$$\lambda = 2d(12/\chi)^m.$$

Then

$$B_1 = (8h(\alpha))^{2d(12/\chi)^{m+1}}.$$

If $h(\alpha) \leqq 4^{10}$, then the second assertion of the theorem follows from the first. If $h(\alpha) > 4^{10}$, then $h(\alpha) > (8h(\alpha))^{1/2}$. Our interval is a window of exponential width not greater than

$$\frac{\log B_1}{\log(8h(\alpha))^{1/2}} = 4d(12/\chi)^{m+1}.$$

We also have $\delta = \mu - 2 > 2.1 - 2 = 1/10$, so that $4^{1/\delta} < 4^{10}$. Then by Lemma 8C, the number of approximations is not greater than

$$1 + \frac{\log(8d(12/\chi))^{m+1}}{\log(\mu - 1)},$$

which is $\ll 1$.

THEOREM 9B. *Suppose α is algebraic of degree $d \geqq 3$, and $0 < \delta < 1$. Then the number of δ-approximations to α is less than*

$$\frac{\log^+ \log h(\alpha)}{L} + c(d, \delta), \tag{9.2}$$

where

$$c(d, \delta) = \frac{10^8}{\delta^5}(\log 2d)^2 \log\left(\left(\frac{50}{\delta}\right)^2 \log 2d\right).$$

This theorem estimates the number of "exceptional" approximations in Roth's Theorem. Davenport and Roth (1956) had given an estimate with a summand $\exp(70d^2\delta^{-2})$. The latest results are by Bombieri and Van der Poorten (1988) and by Luckhardt (1989). Both use the Theorem of Esnault and Viehweg.

In Theorem 9B, the first term in the estimate is best possible (see Theorem 9C below), but the $c(d, \delta)$ term can probably be improved. Actually Bombieri and Van der Poorten had 3000 in place of 10^8, but they also had

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{64y^{2+\delta}}$$

rather than δ-approximations, and had $\delta/2$ in place of $L = \log(1 + \delta) > \delta/2$ in (9.2).

Proof. Put $m = [(50/\delta)^2 \log 2d]$ and $\lambda = 2m^m$. Then $\lambda > d$. Consider "small solutions" to be those with

$$y \leqq (4h(\alpha))^{50\lambda/\delta} = B_2.$$

By Theorem 8D, the number of such approximations is not greater than

$$\frac{\log\log B_2}{L} + 20\left(\frac{1}{\delta} + 1\right).$$

Estimating the first term, we have

$$\log B_2 = \frac{50\lambda}{\delta} \log(4h(\alpha)),$$

so that

$$\log\log B_2 \leqq \log\frac{50}{\delta} + \log\lambda + \log\log 4h(\alpha).$$

We know that

$$\log\lambda < 1 + m\log m \leqq 1 + \left(\left(\frac{50}{\delta}\right)^2 \log 2d\right)\log\left(\left(\frac{50}{\delta}\right)^2 \log 2d\right),$$

and also

$$\log\log 4h(\alpha) \leqq 1 + \log^+ \log h(\alpha).$$

So the total number of "small solutions" is not greater than

$$\frac{\log^+ \log h(\alpha)}{L} + \frac{2((50/\delta)^2 \log 2d)\log((50/\delta)^2 \log 2d)}{\delta/2}.$$

Now consider "large solutions" to be those with $y > B_2$. As in the previous proof, if $\beta = x/y$, then $h(\beta) < 3h(\alpha)^d y$. Consider

$$\begin{aligned} y^{2+\delta} &= y^{2+(\delta/2)} y^{\delta/2} \\ &> h(\beta)^{2+(\delta/2)}(3h(\alpha))^{-3d} y^{\delta/2} \\ &> h(\beta)^{2+(\delta/2)}. \end{aligned}$$

The last inequality follows because $y > B_2$ and $\lambda > d$. So

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}}$$

yields

$$|\alpha - \beta| < \frac{1}{h(\beta)^{2+(\delta/2)}}.$$

Apply Theorem 6B with $\delta/2$ in place of δ. Then either $h(\beta) < B_2$ (which in our case is ruled out) or $h(\beta)$ lies in the union of at most $m-1$ windows of exponential width $C = 6dm\lambda$. Notice that $B_2 \geqq 4^{2/\delta}$, so we can apply Lemma 8C with $\delta/2$ in place of δ. This tells us that the number of approximations with $h(\beta)$ in the given window is not larger than

$$\begin{aligned} \frac{\log 2C}{\log(1+(\delta/2))} + 1 &\leqq \frac{4}{\delta}\log 2C + 1 \\ &< \frac{5}{\delta}\log 2C. \end{aligned}$$

We will estimate $\log 2C$. We know that $2C = 24dm^{m+1}$, so that

$$\log 2C \leqq 2m\log m + \log 24d.$$

Then the number of approximations in a given window is

$$\begin{aligned} &\leqq \frac{10}{\delta} m \log m + \frac{5}{\delta} \log 24d \\ &< \frac{11}{\delta} m \log m. \end{aligned}$$

The number of windows is less than m, so the total number of "large" approximations is less than

$$\frac{11}{\delta} m^2 \log m \leqq \frac{11}{\delta} \left(\frac{50}{\delta}\right)^4 (\log 2d)^2 \log \left(\left(\frac{50}{\delta}\right)^2 \log 2d \right).$$

Combining the results for "small" and "large solutions" gives the desired bound.

THEOREM 9C. *Let K be a real algebraic number field of degree $d \geqq 2$. Let $\delta > 0$ be given. Then there are infinitely many $\alpha \in K$, with $K = \mathbb{Q}(\alpha)$ and $h(\alpha) \geqq e$, such that the number of δ–approximations to α is greater than*

$$\frac{\log \log h(\alpha)}{L} - c_o(K, \delta).$$

Remark. We could drop the condition that $h(\alpha) \geqq e$ if we replace $\log \log h(\alpha)$ with $\log^+ \log h(\alpha)$.

This result is due to Mueller and Schmidt (1989).

Proof. We may choose $\gamma \in K$ with $\mathbb{Q}(\gamma) = K$ and $|\gamma| < 1/2$. We also construct the sequence $\left\{ \frac{p_n}{q_n} \right\}$ as in Theorem 8E. Given $N \geqq 1$, let b_N be the least integer such that $b_N \geqq q_N^{2+\delta}$. Then we may pick an integer a_N with

$$\left| \gamma - \frac{a_N}{b_N} - \frac{p_N}{q_N} \right| < \frac{1}{2b_N} \leqq \frac{1}{2a_N^{2+\delta}}.$$

Set

$$\alpha_N = \gamma - \frac{a_N}{b_N}.$$

Then α_N generates our number field.

Suppose n satisfies $1 \leqq n \leqq N$. Then we have

$$\begin{aligned} \left| \alpha_N - \frac{p_n}{q_n} \right| &\leqq \left| \alpha_N - \frac{p_N}{q_N} \right| + \left| \frac{p_N}{q_N} - \frac{p_n}{q_n} \right| \\ &< \frac{1}{2q_N^{2+\delta}} + \frac{1}{q_n q_{n+1}} \\ &\leqq \frac{1}{2q_N^{2+\delta}} + \frac{1}{2q_N^{2+\delta}} \\ &= \frac{1}{q_N^{2+\delta}}, \end{aligned}$$

where the last inequality follows from the construction of $\left\{\frac{p_n}{q_n}\right\}$ in §8. (Recall, we had $q_{n+1} \geqq 2q_n^{1+\delta}$.) So for $1 \leqq n \leqq N$, we have that p_n/q_n is a δ-approximation to α_N. Hence, α_N has at least N of these δ-approximations.

Now we seek a lower limit for N in terms of $h(\alpha_N)$. We have (see Exercise 7C in Chapter I)

$$\begin{aligned} h(\alpha_N) &= h\left(\gamma - \frac{a_N}{b_N}\right) \\ &\leqq \sqrt{2}\, h(\gamma) h\left(\frac{a_N}{b_N}\right). \end{aligned}$$

Furthermore,

$$\left|\frac{a_N}{b_N}\right| \leqq |\gamma| + \left|\frac{p_N}{q_N}\right| + \frac{1}{2} \leqq 2,$$

so that its height satisfies

$$h\left(\frac{a_N}{b_N}\right) = \sqrt{a_N^2 + b_N^2} \leqq \sqrt{5}\, b_N.$$

We than have

$$\begin{aligned} h(\alpha_N) &\leqq \sqrt{10}\, h(\gamma) b_N \\ &< 2\sqrt{10}\, h(\gamma) q_N^{2+\delta} \end{aligned}$$

since b_N was the least integer with $b_N \geqq q_N^{2+\delta}$. Taking logarithms gives

$$\log h(\alpha) \leqq (2+\delta) \log q_N + c'(K),$$

where the constant depends only on K at this point. By our construction in §8, we know that

$$\log q_N \leqq \frac{(1+\delta)^{N-1}}{\delta} \log 3.$$

Therefore,

$$\log h(\alpha_N) \leqq c''(K,\delta)(1+\delta)^N$$

and

$$N \geqq \frac{\log\log h(\alpha_N)}{L} - c_o(K,\delta).$$

§10. A Generalization of Roth's Theorem.

Let $\mathbb{Q} \subset k \subset K$ be algebraic number fields. As in §I.6, let $M(K)$ be an indexing set for absolute values of K. We write

$$M(K) = M_0(K) \cup M_\infty(K),$$

where $M_0(K)$ consists of non-Archimedean, and M_∞ of the Archimedean absolute values. In most parts of these Notes, S will denote a finite set of the type

$$M_\infty(K) \subset S \subset M(K).$$

However, in the present section we need only that S is a finite subset of $M(K)$. Suppose that for each $v \in S$ we are given a linear form $L_v = L_v(X,Y)$ with coefficients in K. We will study the inequality

$$\prod_{v \in S} \frac{|L_v(\mathbf{x})|_v^{n_v}}{|\mathbf{x}|_v^{n_v}} < H_k(\mathbf{x})^{-2-\varepsilon} \tag{10.1}$$

in unknowns $\mathbf{x} = (x,y)$ with components in k, where $|\mathbf{x}|_v = \max(|x|_v, |y|_v)$ and where n_v is the local degree. Since (10.1) is unaffected if we replace $\mathbf{x}$ by a multiple, $\mathbf{x}$ in projective space $\mathbb{P}^1(k)$.

THEOREM 10A. *Given $\varepsilon > 0$, (10.1) has only finitely many solutions* $\mathbf{x} \in \mathbb{P}^1(k)$.

This is due to Lang (1962). Earlier generalisations of Roth's Theorem were given by Ridout (1958). Now why does this actually give Roth's Theorem?

Suppose α is algebraic, and suppose

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{|y|^{2+\varepsilon}}. \tag{10.2}$$

Then

$$|\alpha y - x| < C_1 |\mathbf{x}|^{-1-\varepsilon}$$

with a constant C_1. Further if $\alpha = \alpha^{(1)}, \dots, \alpha^{(d)}$ are the conjugates of α (in $\mathbb{C}$), then

$$|\alpha^{(1)} y - x| \cdots |\alpha^{(d)} y - x| \leqq C_2 |\mathbf{x}|^{d-2-\varepsilon}.$$

Set $L_v(X,Y) = \alpha Y - X$ for each v Then if $k = \mathbb{Q}$ and $K = \mathbb{Q}(\alpha)$, we have

$$\prod_{v \in M_\infty(K)} |L_v(\mathbf{x})|_v^{n_v} = \prod_{i=1}^{n} |\alpha^{(i)} y - x| \leqq C_2 |\mathbf{x}|^{-2-\varepsilon} = C_2 H_k(\mathbf{x})^{d-2-\varepsilon},$$

or

$$\prod_{v \in M_\infty(K)} \frac{|L_v(\mathbf{x})|_v^{n_v}}{|\mathbf{x}|_v^{n_v}} < C_2 H_k(\mathbf{x})^{-2-\varepsilon}.$$

By Theorem 10A this has only a finite number of solutions, $\mathbf{x} \in \mathbb{P}^1(\mathbb{Q})$, so that (10.2) has only finitely many solutions x/y.

A more quantitative version is as follows.

THEOREM 10B. *Suppose K is of degree δ. Suppose these are not more than t distinct forms L_v for $v \in S$. Define $|L_v|_v$ and $H_K(L_v)$ in terms of the coefficient vectors* *of L_v, and suppose that $H_K(L_v) \leqq H$ for $v \in S$. Then for given $C > 0$, the number of solutions*

$$\prod_{v \in S} \left(\frac{|L_v(\mathbf{x})|_v}{|L_v|_v |\mathbf{x}|_v} \right)^{n_v} < CH_K(\mathbf{x})^{-2-\varepsilon}$$

in $\mathbf{x} \in \mathbb{P}^1(k)$ with

$$H_k(\mathbf{x}) > c_1(\delta, t, \varepsilon)(C + H + 1)^{c_2(\delta,t,\varepsilon)}$$

is less than

$$c_3(\delta, t, \varepsilon) c_4(\varepsilon)^s$$

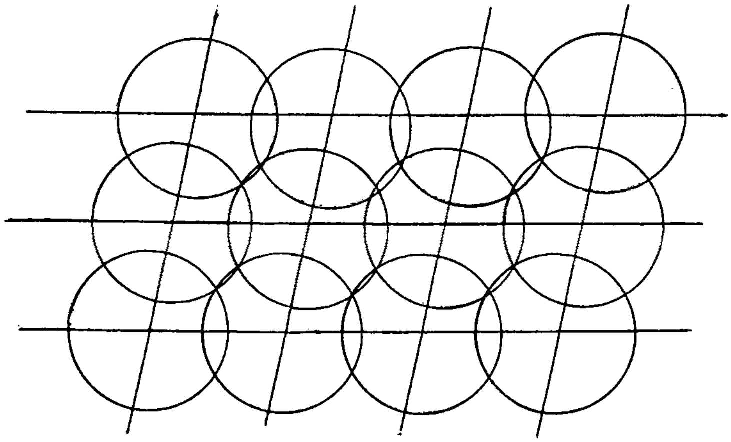
where $s = \operatorname{Card} S$.

As Evertse, Győry, Stewart and Tijdeman (1988) point out, this theorem can be proved by making Lang's arguments more explicit, and combining them with ideas of Davenport and Roth (1955). But no explicit proof of Theorem 10B has been published.

The following exercises are not on the material of this particular section but could have been given earlier.

Exercise 10a. Let B be a symmetric convex body in $\mathbb{R}^n$ and Λ a lattice. The *inhomogeneous minimum* of B with respect to Λ is defined as the least μ such that $\Lambda + \mu B$ covers $\mathbb{R}^n$, (i.e., every $\mathbf{x} \in \mathbb{R}^n$ may be written as $\ell + \mathbf{x}$ with $\ell \in \Lambda$ and $\mathbf{y} \in \mu B$). Prove that μ is well-defined, and that $0 < \mu \leqq n\lambda_n/2$, where λ_n is the nth minimum.

For $n = 2$ and B a disk centered at the origin we have the following picture.



Exercise 10b. Let $\alpha \in \mathbb{R}$ be irrational. We call $(x, y) \in \mathbb{Z}^2$ a *best approximation* to α if y is positive, $|\alpha y - x| < 1/2$, and if for any other pair (x', y') with $1 \leqq y' \leqq y$, we have $|\alpha y' - x'| > |\alpha y - x|$. Show that one gets an infinite sequence of best approximations, say $(x_1, y_1), (x_2, y_2), \ldots$, with $y_1 < y_2 < \cdots$ and

$$|\alpha y_i - x_i| \leqq \frac{1}{y_{i+1}} \qquad (i = 1, 2, \ldots).$$

Exercise 10c. Let $\alpha \in \mathbb{R}$ be irrational, and for $N \geqq 1$, let $\Pi(N)$ be the parallelogram

$$|\alpha y - x| \leqq \frac{1}{N}, \quad |y| \leqq N. \tag{10.3}$$

Since the area of $P(N)$ is 4, Minkowski's Convex Body Theory says that the first minimum satisfies $\lambda_1 = \lambda_1(N) \leqq 1$. Show that there are arbitrarily large values of N with $\lambda_2(N) \leqq 1$. (Hint: This should follow from Exercise 10b.)

Exercise 10d. Combine Exercises 10a and 10c to show that if $\alpha, \beta \in \mathbb{R}$, where α is irrational and β is not of the type $\beta = m\alpha + n$ with $m, n \in \mathbb{Z}$, then there are infinitely many $(x, y) \in \mathbb{Z}^2$ with $y > 0$ and

$$|\alpha y - \beta - x| < 1/y.$$

Remarks. Exercise 10d is a quantitative version of the one-dimensional "Kronecker's Theorem", which only asserts that we can solve

$$|\alpha y - \beta - x| < \varepsilon$$

for α irrational. Minkowski proved that (10.3) may be replaced by the stronger inequality

$$|\alpha y - \beta - x| < 1/(4y),$$

which is best possible. (See Cassels (1957), Chapter III, Theorem II A).

III. The Thue Equation.

References: Thue (1909), A. Baker (1968), Bombieri and Schmidt (1987).

§1. **Main Result.** Let $F(X,Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$ with $a_i \in \mathbb{Z}$ be a form of degree $d \geqq 3$ which is irreducible over $\mathbb{Q}$.

Remark. Such a form F can never be irreducible over $\mathbb{C}$. First consider

$$F(X,1) = a_0X^d + a_1X^{d-1} + \cdots + a_d = a_0(X-\alpha_1)\cdots(X-\alpha_d)$$

with $\alpha_1, \ldots, \alpha_d$ algebraic of degree d and conjugates of one another. Then

$$F(X,Y) = Y^dF\left(\frac{X}{Y}, 1\right) = a_0(X-\alpha_1Y)\cdots(X-\alpha_dY).$$

Theorem 1A. (Thue, 1909). *Let F as above and m be given. The equation*

$$F(x,y) = m \tag{1.1}$$

has only finitely many integer solutions (x,y).

Remark. Today, equations of type (1.1) are called Thue equations.
Remark. Theorem 1A is false for $d = 2$. Consider, for example,

$$x^2 - 2y^2 = 1.$$

This equation factors into

$$(x + \sqrt{2}\,y)(x - \sqrt{2}\,y) = 1.$$

If $\mathfrak{O} = \mathbb{Z}[\sqrt{2}]$, i.e., the ring of elements $x + \sqrt{2}\,y$ with $x, y \in \mathbb{Z}$, then $\varepsilon = x + \sqrt{2}\,y$ and $\hat{\varepsilon} = x - \sqrt{2}\,y$ are units in $\mathfrak{O}$. In particular, we can take $x = 3$ and $y = 2$. Then $\varepsilon_0 = 3 + 2\sqrt{2}$ is a unit. For each $n \geqq 1$, the number ε_0^n is also a unit, which gives a solution $\varepsilon_0^n = x_n + \sqrt{2}\,y_n$ to $x_n^2 - 2y_n^2 = 1$. For example $\varepsilon_0^2 = 17 + 12\sqrt{2}$, so that $x_2 = 17$, $y_2 = 12$.

Proof. Factoring $F(x,y)$ over $\mathbb{C}$, we can write

$$a_0(x-\alpha_1y)\cdots(x-\alpha_dy) = m. \tag{1.2}$$

Then dividing by y^d and taking absolute values gives

$$|a_0|\left|\alpha_1 - \frac{x}{y}\right|\cdots\left|\alpha_d - \frac{x}{y}\right| = \left|\frac{m}{y^d}\right|. \tag{1.3}$$

We have, without loss of generality,

$$|x - \alpha_1y| = \min_{1 \leqq i \leqq d} |x - \alpha_iy|,$$

which is the same as
$$\left|\alpha_1 - \frac{x}{y}\right| = \min_{1 \leqq i \leqq d} \left|\alpha_i - \frac{x}{y}\right|.$$

Also, let
$$\gamma = \frac{1}{2} \min_{i \neq j} |\alpha_i - \alpha_j| > 0.$$

If y is large, then both sides of (1.3) will be small. In particular, $\left|\alpha_1 - \frac{x}{y}\right|$ will be small. For $i \neq 1$, observe that
$$\left|\alpha_i - \frac{x}{y}\right| \geqq |\alpha_i - \alpha_1| - \left|\alpha_1 - \frac{x}{y}\right| \geqq 2\gamma - \gamma = \gamma.$$

Then we have
$$\left|\alpha_1 - \frac{x}{y}\right| \leqq \left|\frac{m}{a_0 \gamma^{d-1} y^d}\right| = \frac{c}{|y|^d}. \tag{1.4}$$

Since $d \geqq 3$, Roth's Theorem implies that there is only a finite number of solutions (x, y).

Exercise 1a. The proof of Liouville's Theorem 1E of Chapter II uses implicitly that $|F(x,y)| \geqq 1$ for integers x, y. (Actually, it uses that $|P(x/y)| \geqq 1/y^d$ for a polynomial $P \in \mathbb{Z}[X]$ of degree d which does not vanish at x/y.) Employ Roth's Theorem to show that for F as in Theorem 1A,
$$|F(x,y)| \geqq c_0(F, \varepsilon)(\max(|x|, |y|))^{d-2-\varepsilon} > 0.$$

Exercise 1b. In Theorem 1A, one may weaken the hypothesis on F. Rather than supposing that F is irreducible over $\mathbb{Q}$, assume that at least three of the complex numbers $\alpha_1, \ldots, \alpha_d$ in (1.2) are distinct.

The methods of Thue, Siegel, and Roth are "ineffective" in the sense that they don't yield a bound $A = A(F, m)$ such that any solution (x, y) satisfies
$$\max(|x|, |y|) \leqq A.$$

Alan Baker (1967) remedied this situation.

Thue's method, however, can be used to give some upper bound on the number of possible solutions. Lewis and Mahler (1961) gave a bound
$$B = B(d, m, H),$$
where $H = \max_{1 \leqq i \leqq d} |a_i|$. For many years, it had been conjectured that a better bound could be obtained. Siegel (1929) conjectured that there should be some $B = B(d, m)$ independent of H. In subsequent work, he proved this for some cases. Evertse (1983) proved the conjecture in his thesis, obtaining the bound
$$7^{15(\binom{d}{3}+1)^2} + 6 \times 7^{2\binom{d}{3}(\nu+1)},$$

where ν is the number of distinct prime factors of m. More recently, Bombieri and Schmidt gave the following result.

THEOREM 1B. (Bombieri and Schmidt, 1987). *Let F and m be given. The number of primitive solutions to the diophantine equation*

$$F(x,y)=m$$

is not greater than

$$c_0 d^{1+\nu},$$

where c_0 is an absolute constant, ν is the number of distinct prime factors of m, and d is the degree of F.

Further advances on the number of solutions were made in recent work of Stewart (to appear).

THEOREM 1C. *Let F and m be given. The number of solutions of the "Thue inequality"*

$$|F(x,y)| \leqq m$$

is

$$\ll dm^{2/d}(1+\log m^{1/d}).$$

In Theorem 1B, consider the case $m=1$. Then we have $F(x,y)=1$ and $\nu=0$. So the number of solutions is $\ll d$. This bound is not bad, as is seen by the following example. Consider

$$x^d + c(x-y)(2x-y)\cdots(dx-y)=1. \tag{1.5}$$

This equation has at least d solutions, namely (1,1), (1,2), ... , $(1,d)$. In fact, if d is even, we have $2d$ solutions. Hence we see that $\ll d$ is best possible. Note that when c is e.g., a prime, then the form in (1.5) is irreducible over $\mathbb{Q}$ by Eisenstein's criterion.

Now let m be arbitrary, say $m=p_1^{z_1}\cdots p_\nu^{z_\nu}$. Then $p_1\cdots p_\nu \leqq m$ and $\log p_1+\log p_2+\cdots+\log p_\nu \leqq \log m$. If we have $p_1<p_2<\cdots<p_\nu$, then $p_i \geqq i+1$ $(i=1,\ldots,\nu)$. Thus $\log 2+\log 3+\cdots+\log(\nu+1) \leqq \log m$, and for m sufficiently large,

$$\nu\log\nu \leqq (1+\varepsilon)\log m.$$

Then, again for $\varepsilon>0$ and m sufficiently large,

$$\nu \leqq \frac{\log m}{\log\log m}(1+\varepsilon).$$

So the number of solutions of $F(x,y)=m$ is

$$\ll d^{1+\nu} \underset{d,\varepsilon}{\ll} m^\varepsilon$$

as $m\to\infty$.

Conjecture. Given a form F as above, the number of solutions of $F(x,y)=m$ is

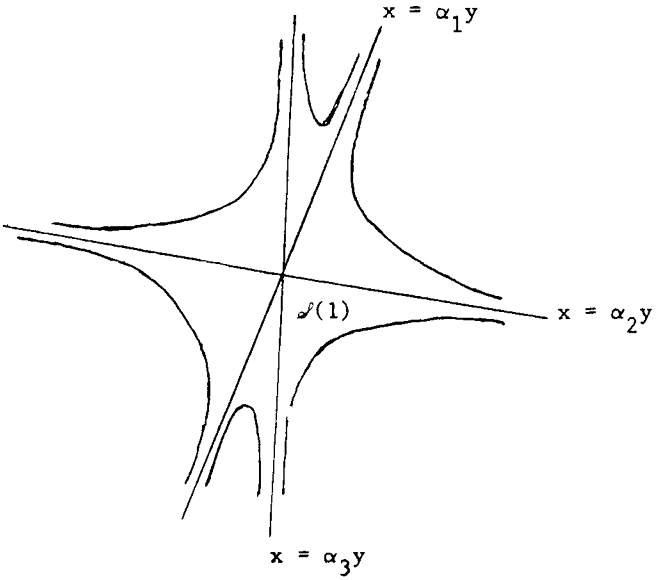
$$\underset{F}{\ll} (\log m)^c,$$

where c is an absolute constant. Perhaps this is valid for $c = 1$, or at least for every $c > 1$.

Now we will look at Theorem 1C. Consider the set $\mathcal{S}(m)$ of $(x, y) \in \mathbb{R}^2$ with

$$|F(x,y)| \leqq m.$$

Then $\mathcal{S}(m) = m^{1/d}\mathcal{S}(1)$. Suppose $F(x,y) = a_0(x - \alpha_1 y)\cdots(x - \alpha_d y)$, and say, for simplicity, that the α_i are real. Then $\mathcal{S}(1)$ contains the lines $x = \alpha_i y$ as in the following illustration.



In Theorem 1C, we are counting the integer points in $\mathcal{S}(m)$. Intuitively, the number should be approximately the area of $\mathcal{S}(m)$. So if $A_F = \text{area}(\mathcal{S}(1))$, the number of solutions should be about $m^{2/d}A_F$.

Remark. Mahler (1934) has shown that the number of solutions of the Thue inequality is

$$\sim A_F m^{2/d}$$

as $m \to \infty$. But the dependency of the error term on the coefficients of F was left unspecified.

§2. Preliminaries. We may deal with a more general type of forms than the forms in 2 variables,

$$F(X,Y) = a_0(X - \alpha^{(1)}Y)\cdots(X - \alpha^{(d)}Y),$$

of §1. Let $L(\mathbf{X})$ be a linear form $\alpha_1 X_1 + \cdots + \alpha_n X_n$ with coefficients in a number field K of degree d. We will suppose that $\alpha_1, \ldots, \alpha_n$ are linearly independent over

$\mathbb{Q}$. If $\alpha \longmapsto \alpha^{(i)}$ $(i = 1, \dots, d)$ are the embeddings of K into $\mathbb{C}$, then let $L^{(i)}(\mathbf{X}) = \alpha_1^{(i)} X_1 + \cdots + \alpha_n^{(i)} X_n$ $(i = 1, \dots, d)$. A *norm form* is a form

$$F(\mathbf{X}) = F(X_1, \dots, X_n) = aL^{(1)}(\mathbf{X}) \cdots L^{(d)}(\mathbf{X})$$

where $a \in \mathbb{Q}^\times$.

If $K \subseteq \mathbb{C}$, put

$$|L| = \sqrt{|\alpha_1|^2 + \cdots + |\alpha_n|^2}\ .$$

The norm form $F(\mathbf{X})$ has rational coefficients, so we may write $F(\mathbf{X}) = a'G(\mathbf{X})$ where $a' \in \mathbb{Q}$ and the coefficients of G are relatively prime integers. Then we have $\operatorname{cont}(F) = |a'|$. We define $H_K(L) = H_K\ (\alpha_1, \dots, \alpha_n)$.

Exercise 2a. Let α be a root of $\alpha^4 - 2\alpha - 2 = 0$ and $K = \mathbb{Q}(\alpha)$. Compute the norm form
$\mathfrak{N}(x + \alpha y + \alpha^2 z) = x^4 + \cdots$.

LEMMA 2A. *Given a norm form* $F(\mathbf{X})$ *(as above), we have*

$$|a||L^{(1)}| \cdots |L^{(d)}| = (\operatorname{cont} F) H_K(L).$$

Proof. Write $M(K) = M_\infty(K) \cup M_0(K)$, where $M_\infty(K)$ consists of Archimedean absolute values (i.e., $v \mid \infty$), and M_0 of non-Archimedean absolute values. We have

$$H_K(L) = \prod_{v \in M(K)} |L|_v^{n_v},$$

where $|L|_v = |(\alpha_1, \dots, \alpha_n)|_v$. Therefore

$$H_K(L) = H_{K\infty}(L) H_{K0}(L) \tag{2.1}$$

where

$$H_{Kj}(L) = \prod_{v \in M_j(K)} |L|_v^{n_v} \quad (j = \infty, 0).$$

By (vi) of Chapter I, §6,

$$H_{K\infty}(L) = |L^{(1)}| \cdots |L^{(d)}|. \tag{2.2}$$

By (vii) of Chapter I, §6, we see that if $\alpha \longmapsto \alpha^{(i)}$ $(i = 1, \dots, d)$ are the isomorphic embeddings of K into $\mathbb{C}$, then

$$H_{K0}(L) = H_{K^{(i)}0}(L^{(i)}) = \prod_{v \in M_0(K^{(i)})} |L^{(i)}|^{n_v} \quad (i = 1, \dots d).$$

Therefore if E is the composition of $K^{(1)}, \dots, K^{(d)}$, then

$$H_{K0}(L) = \prod_{w \in M_0(E)} |L^{(i)}|_w^{n_w/e} \quad (i = 1, \dots d)$$

where $e = [E : K^{(i)}]$ $(i = 1, \dots, d)$. Thus

$$
\begin{aligned}
H_{K0}(L)^{de} &= \prod_{w \in M_0(E)} \left(|L^{(1)}|_w \cdots |L^{(d)}|_w \right)^{n_w} \\
&= \prod_{w \in M_0(E)} |a^{-1}F|_w^{n_w},
\end{aligned}
$$

where in the last relation we used $F = aL^{(1)} \cdots L^{(d)}$ and Gauss' Lemma, and the notation that for any polynomial P, we write $|P|_w$ for the maximum of $|c|_w$ for the coefficients c of P. Since $a^{-1}F$ has rational coefficients,

$$
H_{K0}(L)^{de} = \left(\prod_{p \in M_0(\mathbb{Q})} |a^{-1}F|_p \right)^{de}.
$$

Therefore

$$
H_{K0}(L) = |a| \cdot (\mathrm{Cont}\, F)^{-1}.
$$

This, in conjunction with (2.1), (2.2), gives the assertion.

Recall, $\alpha_1, \dots, \alpha_n$ are linearly independent over $\mathbb{Q}$. So we can extend them to a field basis $\alpha_1, \dots, \alpha_n, \dots, \alpha_d$ of K over $\mathbb{Q}$. Then it is known that the matrix

$$
(\alpha_j^{(i)}) \qquad (1 \leqq i,\ j \leqq d)
$$

is non-singular. Hence the submatrix

$$
(\alpha_j^{(i)}) \qquad (1 \leqq i \leqq d,\ 1 \leqq j \leqq n)
$$

has rank n.

Among the linear forms $L^{(1)}, \dots, L^{(d)}$, there is a set of n linearly independent ones. Let I be the collection of n–tuples $(i_1, \dots, i_n)$ with $1 \leqq i_j \leqq d$ for which the forms $L^{(i_1)}, \dots, L^{(i_n)}$ are linearly independent. The *semi-discriminant* of F is given by

$$
D(F) = |a|^{|I|n/d} \prod_{(i_1, \dots, i_n) \in I} |\det(L^{(i_1)}, \dots, L^{(i_n)})|,
$$

where $|I| = \mathrm{card}\,(I)$. It is easy to see that $D(F)$ is independent of how we write F. Say

$$
F = aL^{(1)} \cdots L^{(d)} = bM^{(1)} \cdots M^{(d)}.
$$

By the essential uniqueness of factorization, we have after reordering that $M^{(i)} = \lambda_i L^{(i)}$ with certain coefficients $\lambda_1, \dots, \lambda_d$. Since $I = I(L^{(1)}, \dots, L^{(d)}) = I(M^{(1)}, \dots, M^{(d)})$, it will suffice (for the independence) that each $L^{(i)}$ occurs exactly $|I|n/d$ times in a determinant of the product. All of the $L^{(i)}$ together occur $|I|n$ times, so if it is "fair", each $L^{(i)}$ will occur $|I|n/d$ times. Since there is an automorphism of E mapping $L^{(1)}$ into $L^{(i)}$, $(1 \leqq i \leqq d)$, each $L^{(i)}$ does indeed occur the same number of times, i.e., $|I|n/d$ times.

Clearly $D(F)$ is nonzero. Because the product is fixed under $\sigma \in Gal(E/\mathbb{Q})$, (where E is the composition of $K^{(1)}, \dots, K^{(d)}$), and since by what we have just said the exponent $|I|n/d$ is an integer, we may conclude that $D(F)$ is rational.

The coefficients of the $L^{(i)}$ lie in the field E. If $v \in M_0(E)$, then by Gauss' Lemma,

$$|a|_v |L^{(1)}|_v \cdots |L^{(d)}|_v = |F|_v.$$

If we suppose that F has integer coefficients, which we shall, then

$$|a|_v |L^{(1)}|_v \cdots |L^{(d)}|_v = |F|_v \leqq 1.$$

On the other hand,

$$|\det(L^{(i_1)}, \dots L^{(i_n)})|_v \leqq |L^{(i_1)}|_v \cdots |L^{(i_n)}|_v.$$

We have noted that each conjugate $L^{(i)}$ occurs exactly $|I|n/d$ times in the product for D. Then for $v \in M_0(E)$, we have

$$|D|_v \leqq (|a|_v |L^{(1)}|_v \cdots |L^{(d)}|_v)^{|I|n/d} \leqq 1.$$

Since this is true for every non-Archimedean $| \ |_v$, we have $D \in \mathbb{Z}$ and $|D| \geqq 1$, where $| \ |$ is the usual absolute value.

If v is Archimedean, then

$$|D|_v \leqq (|a|_v |L^{(1)}|_v \cdots |L^{(d)}|_v)^{|I|n/d}$$

by Hadamard's inequality. So we have

$$|D| \leqq (|a||L^{(1)}| \cdots |L^{(d)}|)^{|I|n/d}$$

for the ordinary absolute value also. We may summarize our results as follows.

LEMMA 2B. *Suppose F is a norm form with coefficients in $\mathbb{Z}$. Then D is a rational integer, $D \neq 0$, and*

$$D(F) \leqq H^*(F)^{|I|n/d},$$

where $H^*(F) = (\text{cont } F) H_K(L) = |a||L^{(1)} \cdots L^{(d)}|$.

Remark. Suppose $n = 2$ and $F = a(X - \alpha^{(1)}Y) \cdots (X - \alpha^{(d)}Y)$ is irreducible over $\mathbb{Q}$. Then $\alpha^{(i)} \neq \alpha^{(j)}$ for $i \neq j$, and I consists of all pairs (i, j) with $i \neq j$ and $1 \leqq i$, $j \leqq d$, so that $|I| = d(d-1)/2$. We may conclude that

$$D(F) \leqq H^*(F)^{d-1}.$$

Now suppose $T : \mathbb{Z}^n \to \mathbb{Z}^n$ is a linear map. Put $F^T(\mathbf{X}) = F(T\mathbf{X})$. Then

$$D(F^T) = |\det T|^{|I|} D(F). \tag{2.3}$$

Note that the set I introduced above depends on the ordering of $L^{(1)},\dots,L^{(d)}$. But its cardinality, which by abuse of notation we denote by $|I(F)|$, depends on F only. For $T \in GL(\text{nonsingular } T, \mathbb{Z})$,

$$|I(F^T)| = |I(F)|.$$

Let p be a prime. Let $T_0, T_1, \dots, T_p$ be the linear maps given by the matrices

$$T_0 = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad T_j = \begin{pmatrix} 1 & 0 \\ j & p \end{pmatrix}, \qquad (j = 1, \dots p).$$

Suppose $\mathbf{x} = \binom{x}{y}$ lies in $\mathbb{Z}^2$. Then either $x \equiv 0 \pmod{p}$ or $x \not\equiv 0 \pmod{p}$. In the first case, $x = px_1$ for some $x_1 \in \mathbb{Z}$ and

$$\begin{pmatrix} x \\ y \end{pmatrix} = T_0 \begin{pmatrix} x_1 \\ y \end{pmatrix}.$$

On the other hand, if $x \not\equiv 0 \pmod{p}$, then $y \equiv jx \pmod{p}$, or $y = jx + py_1$ with $1 \leqq j \leqq p$. In this case,

$$\begin{pmatrix} x \\ y \end{pmatrix} = T_j \begin{pmatrix} x \\ y_1 \end{pmatrix}.$$

We have seen that any integer point $\mathbf{x}$ may be written as

$$\mathbf{x} = T_j \mathbf{x}'$$

for some j, $(0 \leqq j \leqq p)$, and $\mathbf{x}' \in \mathbb{Z}^2$. Further, if $\mathbf{x}$ is primitive, then so is $\mathbf{x}'$. More generally, for n variables, put

$$T_0 = \begin{pmatrix} p & & & & \\ & 1 & & O & \\ & & 1 & & \\ & O & & \ddots & \\ & & & & 1 \end{pmatrix}, \quad T_j = \begin{pmatrix} 1 & 0 & & & & \\ j & p & & & O & \\ & & 1 & & & \\ & & & 1 & & \\ & O & & & \ddots & \\ & & & & & 1 \end{pmatrix}, \quad (1 \leqq j \leqq p).$$

Again, every $\mathbf{x} \in \mathbb{Z}^n$ may be written as $\mathbf{x} = T_j \mathbf{x}'$ for some j and some $\mathbf{x}' \in \mathbb{Z}^n$. In symbols,

$$\mathbb{Z}^n = \bigcup_{j=0}^{p} T_j \mathbb{Z}^n.$$

Suppose that we want to study the number of solutions of the diophantine equation

$$F(\mathbf{x}) = 1.$$

This number is not bigger than the sum of the numbers of solutions of

$$F^{T_j}(\mathbf{x}) = F(T_j \mathbf{x}) = 1$$

for $j = 0, 1, \ldots, p$. Since $D(F^T) = |\det T|^I D(F)$, we know that $D(F^{T_j}) \geqq p^{|I|}$. The following lemma is now obvious.

LEMMA 2C. *Let d be fixed and let $\mathfrak{C}$ be a class of norm forms which is closed under nonsingular substitutions $F : \mathbb{Z}^n \to \mathbb{Z}^n$. Let $N_{\mathfrak{C}}$ be the maximum number of solutions of $F(\mathbf{x}) = 1$ over all F in $\mathfrak{C}$. Let $N_{\mathfrak{C}}\ (p)$ be the maximum number of solutions of $F(\mathbf{x}) = 1$ over all F in $\mathfrak{C}$ with $D(F) \geqq p^{|I|}$. Then*

$$N_{\mathfrak{C}} \leqq (p+1) N_{\mathfrak{C}}\ (p).$$

Remark 2D. The lemma can be modified in two ways. Rather than counting solutions of $F(\mathbf{x}) = 1$, we may count solutions of $F(\mathbf{x}) \in S$, where S is a given set of integers. Secondly, the lemma remains true if instead of counting all integer points we count only primitive integer points.

Now let us restrict to $n = 2$ and $F(X, Y)$ as in Thue's Theorem, and of degree d. Let $N_F(m)$ be the number of integer solutions of the Thue inequality $|F(x, y)| \leqq m$ and $P_F(m)$ the number of primitive integer solutions of the same inequality. Let $P'_F(m)$ be the number of primitive integer solutions of the inequality

$$m/2^d < |F(x, y)| \leqq m. \tag{2.4}$$

Furthermore, let $N(m) = \max\limits_{F} N_F(m)$, and likewise for $P(m)$ and $P'(m)$.

PROPOSITION 2E. *Suppose F is a form as in Thue's Theorem and $D(F) \geqq (50 m^{1/d})^{2|I|}$. Then*

$$P'_F(m) \ll d(1 + \log m^{1/d}),$$

where the implicit constant is absolute.

Proposition 2E will be proven in sections 3, 4, and 5. We will use it now to deduce Theorem 1C.

Proof. (of Theorem 1C). Pick a prime

$$p \geqq 2500 m^{2/d}. \tag{2.5}$$

Then if $D(F) \geqq p^{|I|}$, the condition of Proposition 2E is true. Combining Remark 2D and the proposition, we get that

$$\begin{aligned} P'(m) &\ll (p+1) d (1 + \log m^{1/d}) \\ &\ll d m^{2/d} (1 + \log m^{1/d}), \end{aligned}$$

provided p is a prime chosen as small as possible with (2.5). Given m, pick u satisfying

$$2^{du} \leqq m < 2^{d(u+1)}.$$

Then

$$\begin{aligned} P(m) &\leqq P(2^{d(u+1)}) \\ &= \sum_{j=0}^{u+1} P'(2^{dj}) \\ &\ll d\sum_{j=0}^{u+1} 2^{2j}(1+\log 2^j) \\ &\ll d2^{2u}(1+u) \\ &\ll dm^{2/d}(1+\log m^{1/d}). \end{aligned}$$

Now we can count all the solutions of $|F(x,y)| \leqq m$. Given such a solution, say $(x,y) = t(x',y')$ where (x',y') is primitive and $t > 0$, we have

$$|F(x',y')| \leqq m/t^d,$$

since F is homogeneous of degree d. Thus

$$\begin{aligned} N(m) &\leqq \sum_{t \leqq m^{1/d}} P\left(\frac{m}{t^d}\right) \\ &\ll d\sum_{t=1}^{\infty} \frac{m^{2/d}}{t^2}\left(1+\log\left(\frac{m^{1/d}}{t}\right)\right) \\ &\ll dm^{2/d}(1+\log m^{1/d}). \end{aligned}$$

Before giving a proof of Proposition 2E, we show that we may place additional hypotheses on F by introducing an equivalence relation on forms. If F and G are forms of degree d, we say $F \sim G$ if $G = F^T$ for some $T \in SL(2,\mathbb{Z})$, where $SL(2,\mathbb{Z})$ is the group of one-to-one, linear maps from $\mathbb{Z}^2$ onto itself. The number of solutions of the Thue equation $F(x,y) = m$, or the inequality $|F(x,y)| \leqq m$, depends only on the equivalence class of F. The same is also true for primitive solutions.

Recall that we let $P'_F(m)$ denote the number of primitive solutions of the inequality (2.4). Suppose there is such a solution, say $\mathbf{x}_0 = (x_0, y_0)$. Since $\mathbf{x}_0$ is primitive, there exist integers $x_1, y_1 \in \mathbb{Z}$ with

$$\begin{vmatrix} x_0 & y_0 \\ x_1 & y_1 \end{vmatrix} = 1.$$

Let $G(X,Y) = F(x_0X + x_1Y,\ y_0X + y_1Y)$. Then $G \sim F$ and $G(1,0) = F(x_0,y_0)$. This gives us

$$m/2^d < |G(1,0)| \leqq m.$$

We may, therefore, restrict ourselves to forms F which are *normalized* in the sense that $m/2^d < |F(1,0)| \leqq m$. By writing the form as $F(X,Y) = a(X - \alpha^{(1)}Y)\cdots(X - \alpha^{(d)}Y)$, this inequality becomes

$$m/d^d < |a| \leqq m.$$

We will call F *reduced* if F is normalized and if $H^*(F)$ is minimal among all normalized forms which are equivalent to F. We have seen that Proposition 2E is sufficient to get our bound on the number of solutions of the Thue inequality. Since $D(F)$ and $|I(F)|$ are invariant under substitutions from $SL(2,\mathbb{Z})$, we may restrict ourselves to reduced forms F. In view of $D(F) \geqq (50m^{1/d})^{2|I|}$ and Lemma 2B, we need only concern ourselves with reduced forms having

$$H^*(F) \geqq 50^d m. \tag{2.6}$$

We may also suppose, without loss of generality, that cont $(F) = 1$. For in general, if $F = c\hat{F}$ with cont $(\hat{F}) = 1$, we replace F, m respectively by $\hat{F} = c^{-1}F$, $\hat{m} = c^{-1}m$, so that (2.4) becomes $\hat{m}/2^d < |\hat{F}(\mathbf{x})| \leqq \hat{m}$, and $\hat{F}$ is normalized (with respect to $\hat{m}$) and reduced, and (2.6) changes into $H^*(\hat{F}) \geqq 50^d\hat{m}$.

What we need to prove, then, is the following

PROPOSITION 2F. *Let F be a form as in Thue's Theorem. Suppose F is reduced, cont$(F) = 1$, and (2.6) holds. Then*

$$P'_F(m) \ll d(1 + \log m^{1/d}). \tag{2.7}$$

§3. More on the connection between Thue's Equation and Diophantine Approximations.

Throughout the next few sections, we will let $F(X,Y)$ be a form of degree d as in Thue's Theorem. We will write $f(X) = F(X,1) = a(X - \alpha^{(1)})\cdots(X - \alpha^{(d)})$.

LEMMA 3A. *Suppose we are given (x,y) with $y > 0$. Let α be a root of $f(X)$ with*

$$\left|\alpha - \frac{x}{y}\right| = \min_{1 \leqq i \leqq d} \left|\alpha^{(i)} - \frac{x}{y}\right|. \tag{3.1}$$

Suppose $1 \leqq u \leqq d$ and $f^{(u)}(\alpha) \neq 0$. Then

$$\left|\alpha - \frac{x}{y}\right| \leqq \frac{d}{2}\left(\frac{2^d|F(x,y)|}{|f^{(u)}(\alpha)|y^d}\right)^{1/u}. \tag{3.2}$$

Proof. Let $\mathfrak{S}$ denote any ordered subset of $\{1,2,\ldots,d\}$ of cardinality u. How many such $\mathfrak{S}$ are there? There are

$$d(d-1)\cdots(d-u+1) \leqq d^u.$$

Let $f_{\mathfrak{S}}\ \ (X)$ be defined by

$$f_{\mathfrak{S}}\ \ (X) = a \prod_{\substack{1 \leqq i \leqq d \\ i \notin \mathfrak{S}}} (X - \alpha^{(i)}).$$

Then we have

$$f^{(u)}(X) = \sum_{\mathfrak{S}} f_{\mathfrak{S}}\ \ (X).$$

Therefore, given our α, there is some such $\mathfrak{S}$ with $|f^{(u)}(\alpha)| \leqq d^u |f_{\mathfrak{S}}(\alpha)|$. This $\mathfrak{S}$ will be fixed in the sequel. For any j, where $1 \leqq j \leqq d$, we have by (3.1) that

$$|y(\alpha - \alpha^{(j)})| \leqq |y\alpha - x| + |y\alpha^{(j)} - x| \leqq 2|y\alpha^{(j)} - x|.$$

Now $f_{\mathfrak{S}}(\alpha)$ satisfies

$$\begin{aligned} |y^{d-u} f_{\mathfrak{S}}(\alpha)| &= |a| \prod_{j \notin \mathfrak{S}} |y(\alpha - \alpha^{(j)})| \\ &\leqq 2^{d-u} |a| \prod_{j \notin \mathfrak{S}} |y\alpha^{(j)} - x|, \end{aligned}$$

and $f^{(u)}(\alpha)$ satisfies

$$|y^{d-u} f^{(u)}(\alpha)| \leqq d^u 2^{d-u} |a| \prod_{j \notin \mathfrak{S}} |y\alpha^{(j)} - x|.$$

Multiplication of both sides by $\prod_{j \in \mathfrak{S}} |y\alpha^{(j)} - x|$ gives

$$\left(\prod_{j \in \mathfrak{S}} |y\alpha^{(j)} - x| \right) |y^{d-u} f^{(u)}(\alpha)| \leqq d^u 2^{d-u} |F(x,y)|,$$

so that

$$|y\alpha - x|^u |y^{d-u} f^{(u)}(\alpha)| \leqq d^u 2^{d-u} |F(x,y)|.$$

The assertion (3.2) now easily follows.

In what follows, we will apply the lemma for $u = 1$. For this we need a lower bound for $|f'(\alpha)|$.

LEMMA 3B. *Suppose $f(X) \in \mathbb{Z}[X]$ is of degree d with $\mathrm{cont}(f) = 1$, and is irreducible over $\mathbb{Q}$. Let α be a root of f and $K = \mathbb{Q}(\alpha)$. Then*

$$|f'(\alpha)| \geqq \frac{|D(f)|^{1/2}}{h_K(\alpha)^{d-2}} \geqq \frac{1}{h_K(\alpha)^{d-2}}$$

(where $D(f)$ is the (classical) discriminant of f).

Proof. Write $f(X) = a(X - \alpha^{(1)}) \cdots (X - \alpha^{(d)})$ and suppose $\alpha = \alpha^{(1)}$. We have

$$f'(\alpha) = a(\alpha - \alpha^{(2)}) \cdots (\alpha - \alpha^{(d)})$$

and

$$(f'(\alpha))^2 = \frac{a^{2d-2} \prod_{1 \leqq i<j \leqq d} (\alpha^{(i)} - \alpha^{(j)})^2}{a^{2d-4} \prod_{2 \leqq i<j \leqq d} (\alpha^{(i)} - \alpha^{(j)})^2} = \frac{D(f)}{G},$$

say, where $G = a^{2d-4} \prod_{2 \leqq i<j \leqq d} (\alpha^{(i)} - \alpha^{(j)})^2$. We need to estimate G. We have

$$\begin{aligned} |\alpha^{(i)} - \alpha^{(j)}|^2 &\leqq |\alpha^{(i)}|^2 + |\alpha^{(j)}|^2 + 2|\alpha^{(i)}\alpha^{(j)}| \\ &\leqq (1 + |\alpha^{(i)}|^2)(1 + |\alpha^{(j)}|^2) \end{aligned}$$

since $2|\alpha^{(i)}||\alpha^{(j)}| \leqq 1 + |\alpha^{(i)}|^2|\alpha^{(j)}|^2$. Therefore,

$$\begin{aligned} |G| &\leqq |a|^{2d-4} \prod_{2 \leqq i<j \leqq d} (1 + |\alpha^{(i)}|^2)(1 + |\alpha^{(j)}|^2) \\ &= |a|^{2d-4} \prod_{i=2}^{d} (1 + |\alpha^{(i)}|^2)^{d-2} \\ &\leqq \left(|a|(1 + |\alpha^{(1)}|^2)^{1/2} \cdots (1 + |\alpha^{(d)}|^2)^{1/2} \right)^{2d-4}. \end{aligned}$$

Let $F(X,Y) = a(X - \alpha^{(1)}Y) \cdots (X - \alpha^{(d)}Y) = aL^{(1)}(X) \cdots L^{(d)}(X)$. Then

$$|G| \leqq \left(|a||L^{(1)}| \cdots |L^{(d)}| \right)^{2d-4} = (h_K(\alpha))^{2d-4}$$

by Lemma 2A, since $\operatorname{cont}(F) = 1$ and $H_K(L^{(1)}) = h_K(\alpha)$. The desired result now follows, since

$$|f'(\alpha)|^2 = \left| \frac{D(f)}{G} \right| \geqq \frac{|D(f)|}{(h_K(\alpha))^{2d-4}}.$$

Combining these two results, with $u = 1$ in Lemma 3A, gives the following.

LEMMA 3C. *Let F and f be as above. Suppose*

$$|F(x,y)| \leqq m.$$

If, as before, $y > 0$ and α is among $\alpha^{(1)}, \ldots, \alpha^{(d)}$ with

$$\left| \alpha - \frac{x}{y} \right| = \min_{1 \leqq i \leqq d} \left| \alpha^{(i)} - \frac{x}{y} \right|,$$

then

$$\left| \alpha - \frac{x}{y} \right| \leqq \frac{d}{2} \frac{2^d h_K(\alpha)^{d-2} m}{y^d}.$$

This result is due to Lewis and Mahler (1961).

We now have some reasonably nice values for the constant in (1.4).

§4. Large Solutions.

Recall, we are estimating $P'_F(m)$, i.e., the number of primitive solutions of (2.4):

$$m/2^d < |F(\mathbf{x})| \leqq m.$$

The hypothesis on F in Proposition 2F is that F is reduced with $\operatorname{cont}(F) = 1$ and $H^*(F) \geqq 50^d m$.

If $y = 0$, we have the primitive points (1,0) and $(-1,0)$. By putting another factor in our $\ll$ inequality, we may restrict our solutions to those with $y > 0$. We will let "large solutions" be those with

$$y \geqq H^*(F)^8. \tag{4.1}$$

Write $F(X,Y) = a(X - \alpha^{(1)}Y)\cdots(X - \alpha^{(d)}Y)$ and $L = X - \alpha Y$. Then $H^*(F) = (\mathrm{cont}\,F)H_K(L) = h_K(\alpha) = h_K(\alpha^{(i)})$. Therefore, "large solutions" satisfy $y > (h_K(\alpha^{(i)}))^8$ $(i = 1, \ldots, d)$. By Lemma 3C, some root α satisfies

$$\left|\alpha - \frac{x}{y}\right| < \frac{d}{2}\,\frac{2^d h_K(\alpha)^{d-2} m}{y^d}.$$

Since $h_K(\alpha) \geqq 50^d m$, we have

$$\left|\alpha - \frac{x}{y}\right| < \frac{h_K(\alpha)^d}{y^d} \tag{4.2}$$

with plenty to spare. Since $d \geqq 3$, we have

$$d = \frac{1}{8}d + \frac{7}{8}d > \frac{1}{8}d + \frac{\sqrt{3}}{2}d \geqq \frac{1}{8}d + \frac{3}{2}\sqrt{d}\,.$$

Then (4.2) for large solutions yields

$$\left|\alpha - \frac{x}{y}\right| < \frac{h_K(\alpha)^d}{y^{d/8}y^{3\sqrt{d}/2}} < \frac{1}{y^{3\sqrt{d}/2}}\,. \tag{4.3}$$

As an application of Theorem 9A of Chapter II, we saw that the number of solutions of (4.3) with $y > h(\alpha)$ is $\ll 1$. Here we have $y > h_K(\alpha)^8 \geqq h(\alpha)$. Thus the number of large solutions for the given root α is $\ll 1$. Then the total number of large solutions is $\ll d$. We state this in the following lemma.

LEMMA 4A. *Let F be a form of degree d as in Thue's Theorem. Suppose $\mathrm{cont}(F) = 1$ and $H^*(F) \geqq 50^d m$. Then the number of primitive solutions of (2.4) with $y \geqq H^*(F)^8$ is $\ll d$.*

Thus when it comes to large solutions, the log factor in (2.7) is unnecessary.

§5. Small Solutions. We let small solutions be those with $y < H^*(F)^8$. By Lemma 2F, we may assume that F is reduced (and therefore normalized). We will also assume that

$$H^*(F) \geqq 50^d m. \tag{5.1}$$

LEMMA 5A. *Suppose $G(X,Y) = b_0(X - \beta^{(1)}Y)\cdots(X - \beta^{(d)}Y)$ is normalized and is equivalent to F. Let $\ell \in \mathbb{Z}$ and let*

$$\eta_i = |\beta^{(i)} - \ell| + 1 \qquad (1 \leqq i \leqq d).$$

Then $\eta_1 \cdots \eta_d \geqq Q$, where

$$Q = H^*(F)/m. \tag{5.2}$$

Proof. Let

$$\begin{aligned}\hat{G}(X,Y) &= G(X + \ell Y, Y)\\ &= b_0 \prod_{i=1}^{d}(X - (\beta^{(i)} - \ell)Y).\end{aligned}$$

Then $\hat{G} \sim G \sim F$ and $\hat{G}$ is normalized since G is normalized. Furthermore, since F is reduced, we have

$$\begin{aligned}H^*(F) &\leqq H^*(\hat{G})\\ &= |b_0| \prod_{i=1}^{d} \sqrt{1 + |\beta^{(i)} - \ell|^2}\\ &\leqq m\eta_1 \cdots \eta_d,\end{aligned}$$

since $|b_0| \leqq m$.

LEMMA 5B. *Suppose F is as above and $\mathbf{x}, \mathbf{x}_0$ are primitive solutions of our inequality*

$$m/2^d < |F(\mathbf{x})| \leqq m. \tag{5.3}$$

Then there are numbers $\psi_1, \dots, \psi_d$ (depending on $\mathbf{x}, \mathbf{x}_0, F, m$) such that the following conditions are satisfied:

(i) *for each i, either $\psi_i = 0$ or $1/2d \leqq \psi_i \leqq 1$,*

(ii) $\sum_{i=1}^{d} \psi_i \geqq 1/2$,

(iii) *for each i,*

$$|L_i(\mathbf{x}_0)/L_i(\mathbf{x})| \geqq \left(Q^{\psi_i} - \frac{7}{2}\right) |D(\mathbf{x}_0, \mathbf{x})|,$$

where $L_i(\mathbf{x}) = \alpha^{(i)}y - x$ and

$$D(\mathbf{x}_0, \mathbf{x}) = \begin{vmatrix} x_0 & y_0 \\ x & y \end{vmatrix}.$$

Proof. Since $\mathbf{x}$ is a primitive integer point, we may pick $\mathbf{x}' \in \mathbb{Z}^2$ with $D(\mathbf{x}', \mathbf{x}) = 1$. Then $\mathbf{x}, \mathbf{x}'$ is a basis for $\mathbb{Z}^2$. Therefore,

$$\mathbf{x}_0 = r\mathbf{x} + s\mathbf{x}' \quad \text{with} \quad r, s \in \mathbb{Z}.$$

¿From linear algebra, we have $D(\mathbf{x}_0, \mathbf{x}) = sD(\mathbf{x}', \mathbf{x}) = s$. Then we have

$$\mathbf{x}_0 = r\mathbf{x} + D(\mathbf{x}_0, \mathbf{x})\mathbf{x}'.$$

Now

$$\frac{L_i(\mathbf{x}_0)}{L_i(\mathbf{x})} = r + D(\mathbf{x}_0, \mathbf{x})\frac{L_i(\mathbf{x}')}{L_i(\mathbf{x})} = r - D(\mathbf{x}_0, \mathbf{x})\beta_i, \quad (i = 1, \ldots, d)$$

where $\beta_i = -L_i(\mathbf{x}')/L_i(\mathbf{x})$. Set

$$\begin{aligned} G(V, W) &= F(V\mathbf{x} + W\mathbf{x}') \\ &= a_0 \prod_{i=1}^{d} L_i(V\mathbf{x} + W\mathbf{x}') \\ &= a_0 \prod_{i=1}^{d} (VL_i(\mathbf{x}) + WL_i(\mathbf{x}')) \\ &= b_0 \prod_{i=1}^{d} (V - \beta_i W), \end{aligned}$$

where $b_0 = F(\mathbf{x})$. So G is normalized and $G \sim F$.

Since $\mathbf{x}, \mathbf{x}_0$ are solutions to our original inequality, we have

$$0 < |F(\mathbf{x}_0)/F(\mathbf{x})| < 2^d,$$

or equivalently,

$$0 < \prod_{i=1}^{d} |L_i(\mathbf{x}_0)/L_i(\mathbf{x})| < 2^d.$$

Then at least one factor is no greater than 2, say

$$|L_d(\mathbf{x}_0)/L_d(\mathbf{x})| \leqq 2.$$

Then we have

$$|r - D(\mathbf{x}_0, \mathbf{x})\beta_d| \leqq 2.$$

Putting $\beta = \operatorname{Re}\beta_d$ gives

$$|r - D(\mathbf{x}_0, \mathbf{x})\beta| \leqq 2.$$

Let $\ell \in \mathbb{Z}$ with $|\beta - \ell| \leqq 1/2$. We have

$$\begin{aligned} |L_i(\mathbf{x}_0)/L_i(\mathbf{x})| &= |(\beta - \beta_i)D(\mathbf{x}_0, \mathbf{x}) + r - D(\mathbf{x}_0, \mathbf{x})\beta| \\ &\geqq |\beta - \beta_i||D(\mathbf{x}_0, \mathbf{x})| - 2 \\ &\geqq (|\ell - \beta_i| - \frac{1}{2} - 2)|D(\mathbf{x}_0, \mathbf{x})| \\ &= (\eta_i - \frac{7}{2})|D(\mathbf{x}_0, \mathbf{x})|, \end{aligned}$$

if $\eta_i = |\ell - \beta_i| + 1$. For each i, put

$$\eta_i' = \begin{cases} Q & \text{if} \quad \eta_i \geqq Q, \\ \eta_i & \text{if} \quad Q^{1/2d} \leqq \eta_i < Q, \\ 1 & \text{if} \quad \eta_i < Q^{1/2d}. \end{cases}$$

Define ψ_i by $\eta_i' = Q^{\psi_i}$. By Lemma 5A, we have $\eta_1 \cdots \eta_d \geqq Q$. Therefore, $\eta_1' \cdots \eta_d' \geqq Q^{1/2}$, so that $\sum_{i=1}^{d} \psi_i \geqq 1/2$. Furthermore, $\eta_i \geqq \eta_i' = Q^{\psi_i}$, which gives

$$|L_i(\mathbf{x}_0)/L_i(\mathbf{x})| \geqq \left(Q^{\psi_i} - \frac{7}{2}\right) |D(\mathbf{x}_0, \mathbf{x})|$$

as desired.

In applications of Lemma 5B, we will take $\mathbf{x}_0 = (1, 0)$. This is a solution since F is normalized. In this case, $L_i(\mathbf{x}_0) = -1$ and $D(\mathbf{x}_0, \mathbf{x}) = y$, so the lemma gives $\psi_1, \dots, \psi_d$ satisfying

$$1/|L_i(\mathbf{x})| \geqq \left(Q^{\psi_i} - \frac{7}{2}\right) y \qquad (i = 1, \dots, d).$$

Now suppose that $\psi_i \geqq 1/2d$. Then $Q^{\psi_i} \geqq \sqrt{50} > 7$ by (5.1), (5.2), and

$$1/|L_i(\mathbf{x})| \geqq Q^{\psi_i} y/2 \geqq Q^{\psi_i/2} y \quad (i = 1, \dots, d).$$

That is,

$$|L_i(\mathbf{x})| \leqq 1/Q^{\psi_i/2} y \qquad (i = 1, \dots, d)$$

and

$$\left|\alpha^{(i)} - \frac{x}{y}\right| < 1/Q^{\psi_i/2} y^2 \qquad (i = 1, \dots, d).$$

We state this in the following lemma.

LEMMA 5C. *Suppose F is a form as above (normalized and reduced) and $\mathbf{x} = (x, y)$ is a primitive solution of our inequality, i.e.*

$$m/2^d < |F(x, y)| \leqq m \tag{5.3}$$

with $y > 0$. Then there exist numbers $\psi_i = \psi_i(\mathbf{x})$ $(i = 1, \dots d)$ as above with

$$\left|\alpha^{(i)} - \frac{x}{y}\right| < \frac{1}{Q^{\psi_i/2} y^2} \tag{5.4}$$

for every i in $1 \leqq i \leqq d$ with $\psi_i > 0$.

Compare this with Lemma 3C which says that for some $\alpha^{(i)}$, we have

$$\left|\alpha^{(i)} - \frac{x}{y}\right| < \frac{c}{y^d}.$$

For small values of y, Lemma 5C is better than 3C, because there is no constant in the numerator in (5.4).

LEMMA 5D. *Let $\mathfrak{X}$ be the set of primitive solutions of our inequality (5.3) with $1 \leqq y \leqq Y = H^*(F)^8$. Then for any i, $1 \leqq i \leqq d$, we have*

$$\sum_{\mathbf{x} \in \mathfrak{X}} \psi_i(\mathbf{x}) \ll 1 + \frac{\log Y}{\log Q}.$$

Proof. Given i, let $\mathbf{x}_1, \ldots, \mathbf{x}_\nu$ be the elements of $\mathfrak{X}$ with $\psi_i(\mathbf{x}) > 0$, ordered such that $y_1 \leqq y_2 \leqq \cdots \leqq y_\nu \leqq Y$. Then

$$\begin{aligned} \frac{1}{y_j y_{j+1}} &\leqq \left| \frac{x_j}{y_j} - \frac{x_{j+1}}{y_{j+1}} \right| \\ &\leqq \left| \alpha^{(i)} - \frac{x_j}{y_j} \right| + \left| \alpha^{(i)} - \frac{x_{j+1}}{y_{j+1}} \right| \\ &< \frac{1}{Q^{\psi_i(\mathbf{x}_j)/2} y_j^2} + \frac{1}{Q^{\psi_i(\mathbf{x}_{j+1})/2} y_{j+1}^2} \\ &\leqq \frac{1}{q^{\psi_i(\mathbf{x}_j)/2} y_j^2} + \frac{1}{2 y_j y_{j+1}}. \end{aligned}$$

The last inequality follows from $Q^{\psi_i(\mathbf{x}^{j+1})/2} \geqq Q^{1/4d} \geqq 50^{1/4} > 2$ and $y_{j+1} \geqq y_j$. Now we have

$$\frac{1}{2 y_j y_{j+1}} \leqq \frac{1}{Q^{\psi_i(\mathbf{x}_j)/2} y_j^2},$$

which gives

$$y_{j+1} \geqq Q^{\psi_i(\mathbf{x}_j)/2} y_j / 2 \geqq Q^{\psi_i(\mathbf{x}_j)/4} y_j.$$

(This relationship between y_j and y_{j+1} can be thought of as a "variable gap principle".) Since we have $y_\nu / y_1 \leqq Y$, this gap principle tells us that

$$\prod_{j=1}^{\nu-1} Q^{\psi_i(\mathbf{x}_j)/4} \leqq Y,$$

and therefore

$$\sum_{j=1}^{\nu-1} \psi_i(\mathbf{x}_j) \leqq 4 \frac{\log Y}{\log Q}.$$

Since $\psi_i(\mathbf{x}_\nu) \leqq 1$, the lemma follows.

We are now able to estimate the cardinality of $\mathfrak{X}$. ¿From Lemmas 5B (ii) and 5D, we have

$$\begin{aligned} \frac{1}{2} |\mathfrak{X}| &\leqq \sum_{i=1}^{d} \sum_{\mathbf{x} \in \mathfrak{X}} \psi_i(\mathbf{x}) \\ &\ll d \left(1 + \frac{\log Y}{\log Q} \right) \\ &= d \left(1 + \frac{\log H^*(F)^8}{\log Q} \right). \end{aligned}$$

Therefore, on using (5.1), (5.2), we obtain

$$\begin{aligned}|\mathfrak{X}| &\ll d\left(1+\frac{\log m}{\log Q}\right)\\ &\ll d\left(1+\frac{\log m}{d}\right)\\ &= d(1+\log m^{1/d}).\end{aligned}$$

We have proven, then, the Proposition, and therefore the main result (Theorem 1C), which said that the number of solutions of the Thue inequality $|F(\mathbf{x})| \leqq m$ is

$$\ll dm^{2/d}(1+\log m^{1/d}).$$

In particular, the number of solutions of $F(\mathbf{x}) = 1$ is $\ll d$.

Remark. One might believe that the number of solutions could be estimated in terms of the number of *real* $\alpha^{(i)}$'s, rather than d. This is not the case, as shown by the following.

Example. Let $F(X,Y) = X^d + c(X-Y)^2(2X-Y)^2\cdots(\frac{d}{2}X-Y)^2$, where $c > 0$, and d is even. Then $F(x,y) = 0$ for real x, y would imply that $x = y = 0$. So $F(x,1)$ has no real root. However, $F(x,y) = 1$ has d non-trivial integer solutions, namely $\pm(1,1), \pm(1,2), \dots, \pm(1,\frac{d}{2})$. This example was communicated to me by M. Waldschmidt.

§6. How to Go from $F(\mathbf{x}) = 1$ to $F(\mathbf{x}) = m$. We now know that the equality $F(\mathbf{x}) = 1$ has $\ll d$ solutions. We want to extend our results to Theorem 1B, which states that $F(\mathbf{x}) = m$ has $\ll d^{1+\nu}$ solutions, where $\nu = \nu(m)$ is the number of distinct prime factors of m.

To consider this problem, we go to a wider setting. Consider forms $F(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ which are *decomposable*, i.e., $F = L_1 \cdots L_d$ where $L_1, \dots, L_d$ are linear forms in n variables with complex coefficients.

Exercise 6a. Let F be decomposable as above. Show that F can be written as a product $L_1 \cdots L_d$, where now the coefficients of each L_i generate an algebraic number field K_i of degree $[K_i : \mathbb{Q}] \leqq d$.

For given n and d, let $\mathfrak{C}$ be a class of decomposable forms which is closed in the following sense. If $F \in \mathfrak{C}$ and $G = cF^T$ with c a non-zero rational, $T \in GL(n,\mathbb{Z})$, and $G \in \mathbb{Z}[X_1, \dots, X_n]$, then $G \in \mathfrak{C}$ also.

Example. Suppose $n = 2$ and $\mathfrak{C}$ the class of forms of given degree $d \geqq 3$ and irreducible over $\mathbb{Q}$, as in Thue's equation. Then this class is closed, since irreducibility is unchanged under a linear transformation.

Example. Suppose $F = aL^{(1)} \cdots L^{(d)}$ is a norm form where any n among $L^{(1)}, \dots, L^{(d)}$ are linearly independent. Then this class is also closed.

For a given class $\mathfrak{C}$, let $M_{\mathfrak{C}}\ (1)$ be the maximum number of solutions of $F(\mathbf{x}) = 1$ with $\mathbf{x} \in \mathbb{Z}^n$, where the maximum is over all $F \in \mathfrak{C}$. Let $M_{\mathfrak{C}}\ (m)$ be the maximum number of primitive solution of $F(\mathbf{x}) = m$ over all $F \in \mathfrak{C}$. It is trivial that $M_{\mathfrak{C}}\ (m) = M_{\mathfrak{C}}\ (-m)$.

THEOREM 6A. *If $M_{\mathfrak{C}}\ (1)$ is finite, then*

$$M_{\mathfrak{C}}\ (m) \leqq \binom{d}{n-1}^{\nu} d_{n-1}(m^d) M_{\mathfrak{C}}\ (1),$$

where $\nu = \nu(m)$ is the number of distinct prime factors of m, and $d_{n-1}(x)$ is the number of ways of writing $x = x_1 x_2 \cdots x_{n-1}$ with $x_i \in \mathbb{N}$, $(i = 1, \ldots, n-1)$.

This result has its genesis in Bombieri and Schmidt (1987), where the case $n = 2$ was shown.

Remark. The function $d_2(x)$ is the ordinary divisor function, while $d_1(x) = 1$. In the special case $n = 2$, we have

$$M_{\mathfrak{C}}\ (m) \leqq d^{\nu} M_{\mathfrak{C}}\ \ (1).$$

Furthermore, for the Thue equation, we know that $M_{\mathfrak{C}}\ (1) \ll d$, so that

$$M_{\mathfrak{C}}\ (m) \ll d^{\nu+1},$$

and Theorem 1B is proved.

Exercise 6b. Given n and d, let

$$g(m) = \binom{d}{n-1}^{\nu(m)} d_{n-1}(m^d).$$

Show that $g(m)$ is *multiplicative*, i.e., $g(m_1 m_2) = g(m_1) g(m_2)$ if $\gcd(m_1, m_2) = 1$.

Exercise 6c. Given n, d and $\varepsilon > 0$, and for $g(m)$ as above, show that $g(m) \underset{d,n,\varepsilon}{\ll} m^{\varepsilon}$ as $m \to \infty$.

Because of the multiplicativity of $g(m)$, it will suffice to prove the following.

PROPOSITION 6B. *For $k > 0$ and a prime power p^u where $u \geqq 1$ and $p \mid k$, we have*

$$M_{\mathfrak{C}}\ (kp^u) \leqq \binom{d}{n-1} d_{n-1}(p^{ud}) M_{\mathfrak{C}}\ (k)$$

In what follows, suppose that E is a field and $|\ |$ is a non-Archimedean absolute value on E, sometimes called an *ultra-metric* absolute value. For $\mathbf{x} = (x_1, \ldots, x_n) \in E^n$, put $|\mathbf{x}| = \max(|x_1|, \ldots, |x_n|)$. Similarly, if $P(X_1, \ldots, X_n)$ is a polynomial with coefficients in E, then put $|P| = \max |c|$, over all coefficients c of P.

LEMMA 6C. *Suppose such a field E is algebraically closed. Then*

$$\max_{\substack{\mathbf{x}\in E^n \\ |\mathbf{x}|\leqq 1}} |P(\mathbf{x})| = |P|.$$

Proof. It is clear from the properties of a non-Archimedean absolute value that

$$\max_{\substack{\mathbf{x}\in E^n \\ |\mathbf{x}|\leqq 1}} |P(\mathbf{x})| \leqq |P|.$$

Thus it will suffice to show that there is an $\mathbf{x} \in E^n$ with $|\mathbf{x}| = 1$ and $|P(\mathbf{x})| = |P|$.

Consider the case $n = 1$. We may suppose that $P \neq 0$. Then write $P(X) = P_1(X) + P_2(X)$, where P_1 is the sum of the monomials of P whose coefficients have norm $|P|$, and P_2 is the sum of the remaining monomials. Suppose that

$$P_1(X) = c_{i_1}X^{i_1} + c_{i_2}X^{i_2} + \cdots + c_{i_t}X^{i_t}$$

with $i_1 < \cdots < i_t$. Choose $x \in E$ with

$$P_1(x) = c_{i_t}x^{i_t+1}.$$

Then $|x| = 1$. For if $|x| > 1$, the summand $c_{i_t}x^{i_t+1}$ would dominate, and if $|x| < 1$, the summand $c_{i_1}x^{i_1}$ would dominate. We have

$$|P_1(x)| = |c_{i_t}| = |P|$$

and

$$|P_2(x)| < |P|.$$

Therefore, by the isosceles triangle principle for non-Archimedean absolute values, we have

$$|P(x)| = |P|,$$

as desired.

The general case follows by induction on n.

Remark. The hypothesis of algebraic closure was really necessary, as illustrated by the following example.

Example. Let E be the field of rational numbers with $|\ | = |\ |_p$, the p-adic absolute value associated with some prime p. Let $P = X^p - X$. Then $|P| = 1$. Suppose $x \in \mathbb{Q}$ and $|x| \leqq 1$. Write $x = u/v$ with $u, v \in \mathbb{Z}$ and $p \mid v$. Then

$$x^p - x = \left(\frac{u}{v}\right)^p - \left(\frac{u}{v}\right) = \frac{u^p - uv^{p-1}}{v^p}.$$

The numerator satisfies $u^p - uv^{p-1} \equiv u^p - u \equiv 0 \pmod{p}$. Therefore, $|x^p - x| \leqq 1/p$ and

$$\max_{\substack{x\in \mathbb{Q} \\ |x|\leqq 1}} |P(x)| \leqq \frac{1}{p}.$$

LEMMA 6D. *Let E be a field, not necessarily algebraically closed, with a non-Archimedean absolute value $|\ |$. Let $L_1(\mathbf{X}), \ldots, L_t(\mathbf{X})$ be linearly dependent linear forms with coefficients in E. Given non-negative real numbers $\lambda_1, \ldots, \lambda_t$, let $\mathfrak{K}$ be the set of $\mathbf{x}$ with components in E and satisfying*

$$|L_i(\mathbf{x})| \leqq \lambda_i \quad (i = 1, \ldots, t). \tag{6.1}$$

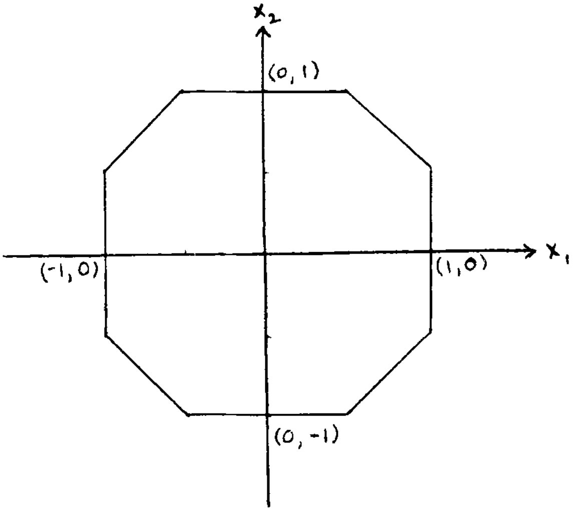
Then $\mathfrak{K}$ may be defined by $t-1$ of these inequalities, i.e., there exists an i_0, $1 \leqq i_0 \leqq t$, such that $\mathfrak{K}$ is defined by

$$|L_i(\mathbf{x})| \leqq \lambda_i \qquad (i = 1, \ldots, i_0 - 1, i_0 + 1, \ldots, t).$$

Remark. This does not hold in the Archimedean case. Consider, for example, the field of real numbers $\mathbb{R}$ with the usual Archimedean absolute value and the system of inequalities

$$|x_1| \leqq 1, \ |x_2| \leqq 1, \ |x_1 + x_2| \leqq 3/2.$$

The corresponding linear forms are clearly linearly dependent. However, the solution set (shown below) cannot be defined with less than three inequalities.



Proof. Since $L_1, \ldots, L_t$ are linearly dependent, there is a non-trivial relation

$$\gamma_1 L_1 + \cdots + \gamma_t L_t = 0,$$

with $\gamma_i \in E$ $(i = 1, \ldots, t)$. Furthermore, not all of the γ_i's are zero, say $\gamma_1 \neq 0, \ldots, \gamma_\ell \neq 0$, but $\gamma_{\ell+1} = \cdots = \gamma_t = 0$. Without loss of generality, we have

$$|\gamma_1|\lambda_1 = \max(|\gamma_1|\lambda_1, \ldots, |\gamma_\ell|\lambda_\ell).$$

Now take $i_0 = 1$. If (6.1) holds for $i = 2, \dots, t$, then the linear relation gives

$$\begin{aligned} |\gamma_1 L_1(\mathbf{x})| &\leqq \max(|\gamma_2||L_2(\mathbf{x})|, \dots, |\gamma_\ell||L_\ell(\mathbf{x})|) \\ &\leqq \max(|\gamma_2|\lambda_2, \dots, |\gamma_\ell|\lambda_\ell) \\ &\leqq |\gamma_1|\lambda_1, \end{aligned}$$

so that $|L_1(\mathbf{x})| \leqq \lambda_1$, and the proof is complete.

LEMMA 6E. *Let E and $|\ |$ be as above. Let $L_1, \dots, L_n$ be n linear forms in n variables with coefficients in E. Let non-negative $\lambda_1, \dots, \lambda_n$ be given. Suppose there is an $\mathbf{x}' \in E^n$ with*

$$|\mathbf{x}'| = 1, \quad |L_i(\mathbf{x}')| \leqq \lambda_i \quad (i = 1, \dots, n).$$

Then there exists an i_0, $1 \leqq i_0 \leqq n$, such that any $\mathbf{x}$ satisfying

$$|\mathbf{x}| \leqq 1, \quad |L_i(\mathbf{x})| \leqq \lambda_i \quad (i = 1, \dots, i_0 - 1, i_0 + 1, \dots, n), \tag{6.2}$$

has in fact

$$|L_i(\mathbf{x})| \leqq \lambda_i \qquad (i = 1, \dots, n).$$

Proof. By the preceding lemma, we may suppose that $L_1, \dots, L_n$ are linearly independent. Then each coordinate X_i may be written as a linear combination of the linear forms $L_1, \dots, L_n$. That is,

$$X_i = \gamma_{i1} L_1(\mathbf{X}) + \dots + \gamma_{in} L_n(\mathbf{X}), \quad (i = 1, \dots, n),$$

with $\gamma_{ij} \in E$ for $1 \leqq i,\ j \leqq n$. Without loss of generality,

$$|\gamma_{11}|\lambda_1 = \max_{1 \leqq i,j \leqq n} |\gamma_{ij}|\lambda_j.$$

The given $\mathbf{x}'$ has

$$|x_i'| \leqq \max_j |\gamma_{ij}|\lambda_j \leqq |\gamma_{11}|\lambda_1,$$

and since $|\mathbf{x}'| = 1$, this gives us $1 \leqq |\gamma_{11}|\lambda_1$. In particular, $\gamma_{11} \neq 0$.

Now we will show that $i_0 = 1$ works. Suppose $\mathbf{x}$ satisfies (6.2). Then the linear expression for the first coordinate gives

$$\begin{aligned} |\gamma_{11}||L_1(\mathbf{x})| &\leqq \max(|\gamma_{12}||L_2(\mathbf{x})|, \dots, |\gamma_{1n}||L_n(\mathbf{x})|, |x_1|) \\ &\leqq \max(|\gamma_{12}|\lambda_2, \dots, |\gamma_{1n}|\lambda_n, |x_1|) \\ &\leqq |\gamma_{11}|\lambda_1 \end{aligned}$$

since $|x_1| \leqq |\mathbf{x}| \leqq 1 \leqq |\gamma_{11}|\lambda_1$. Dividing by $|\gamma_{11}|$ in the inequality gives $|L_1(\mathbf{x})| \leqq \lambda_1$, and the lemma is proved.

LEMMA 6F. *For $d \geqq n$, let $L_1(\mathbf{X}), \dots, L_d(\mathbf{X})$ be d linear forms in n variables with coefficients in E. Let non-negative real numbers $\lambda_1, \dots, \lambda_d$ be given. Suppose* *there is an* $\mathbf{x}' \in E^n$ *with*

$$|\mathbf{x}'| = 1, \quad |L_i(\mathbf{x}')| \leqq \lambda_i \quad (i = 1, \dots , d).$$

Then there are $n - 1$ *among these forms, say* $L_{i_1}, \dots , L_{i_{n-1}}$, *such that any* $\mathbf{x} \in E^n$ *satisfying*

$$|\mathbf{x}| \leqq 1, \quad |L_{i_j}(\mathbf{x})| \leqq \lambda_{i_j} \quad (j = 1, \dots , n - 1)$$

also has

$$|L_i(\mathbf{x})| \leqq \lambda_i \qquad (i = 1, \dots , d).$$

Proof. Apply Lemma 6D repeatedly, $d - n$ times, to reduce the system to n linear forms. Then apply Lemma 6E to reduce further to $n - 1$ forms.

For the following exercises, suppose that E is a field with a non-Archimedean absolute value $|\ |$, as before. Furthermore, suppose that E is complete, i.e., any Cauchy sequence has a limit in E with respect to the absolute value. A set $\mathfrak{K}$ in E^n is called *symmetric, convex* if $\lambda\mathbf{x} + \mu\mathbf{y} \in \mathfrak{K}$ for every $\mathbf{x}, \mathbf{y} \in \mathfrak{K}$ and $|\lambda| \leqq 1$, $|\mu| \leqq 1$. Given $\mathbf{x}_1, \dots , \mathbf{x}_n \in \mathfrak{K}$, their **convex hull** is the set of all points $\lambda_1\mathbf{x}_1 + \cdots + \lambda_n\mathbf{x}_n$ with $|\lambda_i| \leqq 1$, $(i = 1, \dots , n)$. This is simply the smallest convex, symmetric set containing $\mathbf{x}_1, \dots , \mathbf{x}_n$.

Exercise 6d. Suppose $\mathfrak{K} \subseteq E^n$ is a symmetric, convex set, as above. Suppose als that $\mathfrak{K}$ is sequentially compact (i.e., every sequence in $\mathfrak{K}$ has a convergent subsequence) and that $\mathfrak{K}$ contains n linearly independent points. Show that $\mathfrak{K}$ is the convex hull of certain n linearly independent points.

Exercise 6e. Suppose $\mathfrak{K}$ is as in Exercise 6d. Show that there are n linearly independent linear forms $L_1, \dots , L_n$ with coefficients in E such that $\mathfrak{K}$ may be defined by the inequalities

$$|L_i(\mathbf{x})| \leqq 1 \qquad (i = 1, \dots , n).$$

Returning to Proposition 6B, we want to consider the number of primitive solutions of

$$F(\mathbf{x}) = kp^u, \quad \text{where} \quad p \mid k. \tag{6.3}$$

By a previous exercise, we write $F(\mathbf{X}) = L_1(\mathbf{X}) \cdots L_d(\mathbf{X})$, where the coefficients of L_i lie in a field K_i. Let E be the algebraic closure of $\mathbb{Q}$ and let $|\ |$ on E be some extension of the p-adic absolute value $|\ |_p$. With any primitive solution $\mathbf{x}'$ of (6.3), we will associate real numbers $\lambda_1, \dots , \lambda_d$ such that

$$|L_i(\mathbf{x}')| = \lambda_i \qquad (i = 1, \dots , d).$$

Since $\mathbf{x}'$ is primitive, we have $|\mathbf{x}'|_p = 1$. Therefore, by Lemma 6F, given such an $\mathbf{x}'$, we can pick $n - 1$ of the forms, say $L_{i_1}, \dots , L_{i_{n-1}}$, such that any $\mathbf{x} \in E$ with

$$|\mathbf{x}| \leqq 1, \quad |L_{i_j}(\mathbf{x})| \leqq \lambda_{i_j} \quad (j = 1, \dots , n - 1)$$

also satisfies

$$|L_i(\mathbf{x})| \leqq \lambda_i \qquad (i = 1, \dots , n).$$

With each $\mathbf{x}'$, we associate $(L_{i_1},\dots,L_{i_{n-1}};\lambda_{i_1},\dots,\lambda_{i_{n-1}})$, which will be called the *anchor* of $\mathbf{x}'$. Initially, we will count the number of solutions with a given anchor.

Without loss of generality, consider solutions with the anchor $(L_1,\dots,L_{n-1};$ $\lambda_1,\dots,\lambda_{n-1})$. Such an anchor is associated with $\mathbf{x}'$ and $\lambda_1,\dots,\lambda_d$ satisfying

$$\lambda_1\cdots\lambda_d = |L_1(\mathbf{x}')\cdots L_d(\mathbf{x}')| = |kp^u| = p^{-u}.$$

Suppose some $\mathbf{x}\in E^n$ is a solution to the inequalities

$$|\mathbf{x}| \leqq 1 \quad\text{and}\quad |L_i(\mathbf{x})| \leqq \lambda_i \quad (i=1,\dots,n-1). \tag{6.4}$$

By Lemma 6F, such an $\mathbf{x}$ also satisfies

$$|L_i(\mathbf{x})| \leqq \lambda_i \quad (i=1,\dots,d).$$

Thus

$$|F(\mathbf{x})| = |L_1(\mathbf{x})\cdots L_d(\mathbf{x})| \leqq \lambda_1\cdots\lambda_d = p^{-u}.$$

Now, the points $\mathbf{x}\in\mathbb{Z}^n$ with

$$|L_i(\mathbf{x})| \leqq \lambda_i \qquad (i=1,\dots,n-1)$$

make up a lattice. Choose some basis for this lattice, say $\mathbf{a}_1,\dots,\mathbf{a}_n$. Consider $\mathbf{x} = y_1\mathbf{a}_1+\cdots+y_n\mathbf{a}_n$ where $y_i\in E$ and $|y_i|\leqq 1$ $(i=1,\dots,n)$. For such an $\mathbf{x}$, we have (6.4), namely

$$|\mathbf{x}| \leqq 1 \quad\text{and}\quad |L_i(\mathbf{x})| \leqq \lambda_i \quad (i=1,\dots,n-1),$$

therefore

$$|F(\mathbf{x})| \leqq p^{-u}$$

as above. Furthermore, if $\mathbf{x}\in\mathbb{Z}^n$ belongs to our anchor, then $\mathbf{x}$ is in this lattice, i.e.

$$\mathbf{x} = y_1\mathbf{a}_1+\cdots+y_n\mathbf{a}_n. \tag{6.5}$$

We introduce another form G by $G(Y_1,\dots,Y_n) = F(Y_1\mathbf{a}_1+\cdots+Y_n\mathbf{a}_n)$. If $\mathbf{x}$ satisfies $F(\mathbf{x}) = kp^u$ and (6.5), then $G(\mathbf{y}) = kp^u$, where $y = (y_1,\dots,y_n)$ from (6.5). But for any $\mathbf{y}\in E^n$ with $|\mathbf{y}|\leqq 1$, we have $|G(\mathbf{y})|\leqq p^{-u}$. Hence, $|G|\leqq p^{-u}$, by Lemma 6A. We know, then, that every coefficient of G is divisible by p^u. Set $G(\mathbf{Y}) = p^uR(\mathbf{Y})$ with $R(\mathbf{Y})\in\mathbb{Z}[\mathbf{Y}]$. Then $G(\mathbf{y}) = kp^u$ becomes $R(\mathbf{y}) = k$. Furthermore, $R\in\mathfrak{C}$, so the number of solutions to $R(\mathbf{y}) = k$ is not greater than $M_{\mathfrak{C}}(k)$.

We may conclude, then, that the number of solutions with a given anchor is not greater than $M_{\mathfrak{C}}(k)$. It remains for us to estimate the number of possible anchors $(L_{i_1},\dots,L_{i_{n-1}};\lambda_{i_1},\dots,\lambda_{i_{n-1}})$. The number of choices for $(n-1)$-tuples, i.e., $(i_1,\dots,i_{n-1})$, is $\binom{d}{n-1}$. Given $i_1,\dots,i_{n-1}$, how many possibilities exist for $\lambda_{i_1},\dots,$ $\lambda_{i_{n-1}}$? Without loss of generality, we may consider the number of anchors of the form $(L_1,\dots,L_{n-1};\lambda_1,\dots,\lambda_{n-1})$. To answer our question, it is necessary to count the number of possibilities for $\lambda_1,\dots,\lambda_{n-1}$.

We begin by making several observations.

(i) By Gauss' Lemma, we have $|L_1| \cdots |L_d| = |F| \leqq 1$. Suppose $\lambda_1, \ldots, \lambda_{n-1}$ belongs to an anchor coming from $\lambda_1, \ldots, \lambda_d$. Then $\lambda_1 \cdots \lambda_d = p^{-u}$. Putting $\mu_i = \lambda_i / |L_i|$, we have

$$\mu_i \leqq 1 \qquad (i = 1, \ldots, d)$$

and

$$\mu_1 \cdots \mu_d \geqq p^{-u}.$$

(ii) If $\lambda_1, \ldots, \lambda_{n-1}$ and $\lambda'_1, \ldots, \lambda'_{n-1}$ both occur in anchors and if $\lambda_i \leqq \lambda'_i$ $(i = 1, \ldots, n-1)$, then $\lambda_i = \lambda'_i$ $(i = 1, \ldots, n-1)$. For suppose $\lambda_1, \ldots, \lambda_{n-1}$ comes from $\lambda_1, \ldots, \lambda_d$ and $\lambda'_1, \ldots, \lambda'_{n-1}$ comes from $\lambda'_1, \ldots \lambda'_d$. Then there must be $\mathbf{x}$ and $\mathbf{x}'$ with $|\mathbf{x}| = |\mathbf{x}'| = 1$, $|L_i(\mathbf{x})| = \lambda_i$, and $|L_i(\mathbf{x}')| = \lambda'_i$. Therefore

$$|\mathbf{x}| = 1 \quad \text{and} \quad |L_i(\mathbf{x})| \leqq \lambda'_i \quad (i = 1, \ldots, n-1).$$

Since $\lambda'_1, \ldots, \lambda'_{n-1}$ belong to an anchor, we have

$$|L_i(\mathbf{x})| \leqq \lambda'_i \qquad (i = 1, \ldots, d),$$

and thus,

$$\lambda_i \leqq \lambda'_i \qquad (i = 1, \ldots, d).$$

However,

$$\lambda_1 \cdots \lambda_d = \lambda'_1 \cdots \lambda'_d = p^{-u};$$

therefore

$$\lambda_i = \lambda'_i \qquad (i = 1, \ldots, d).$$

(iii) Recall that, for each i, the field K_i is an algebraic extension of $\mathbb{Q}$ of degree $\leqq d$. The p-adic absolute value $|\ |_p$ on $\mathbb{Q}$ has the value set $\{p^m : m \in \mathbb{Z}\}$. Since the absolute value $|\ |_v$ on K_i is an extension of $|\ |_p$, we know that it has the value set $\{p^{m/e_i} : m \in \mathbb{Z}\}$, where $e_i = e_i(K_i)$ and $1 \leqq e_i \leqq \deg K_i \leqq d$. (This e_i is known as the *ramification index.*)

Given a primitive solution $\mathbf{x}$, for each i we have $\lambda_i = |L_i(\mathbf{x})|$. From observation (iii), λ_i is of the type p^{m/e_i} for some $m \in \mathbb{Z}$. Then write

$$\mu_i = \frac{\lambda_i}{|L_i|_v} = p^{-v_i/e_i}$$

for some $v_i \in \mathbb{Z}$. We have $v_i \geqq 0$ $(i = 1, \ldots, n-1)$ and $\mu_1 \cdots \mu_{n-1} \geqq p^{-u}$ by observation (i). Hence

$$\frac{v_1}{e_1} + \cdots + \frac{v_{n-1}}{e_{n-1}} \leqq u.$$

Suppose two different anchors have $v_1, \ldots, v_{n-1}$ and $v'_1, \ldots v'_{n-1}$ with $v_i \leqq v'_i$ $(i = 1, \ldots, n-1)$. By applying observation (ii) to the corresponding $\lambda_1, \ldots, \lambda_{n-1}$ and $\lambda'_1, \ldots, \lambda'_{n-1}$, we find that $v_i = v'_i$ $(i = 1, \ldots, n-1)$. Therefore, v_{n-1} is unique once $v_1, \ldots, v_{n-2}$ are given.

It remains, then, to count the number of non-negative $v_1, \ldots, v_{n-2}$ with

$$\frac{v_1}{e_1} + \cdots + \frac{v_{n-2}}{e_{n-2}} \leqq u.$$

Since $e_i \leqq d$, this number is bounded by the number of non-negative $v_1, \ldots, v_{n-2}$ with $v_1 + \cdots + v_{n-2} \leqq du$, which in turn equals the number of non-negative $v_1, \ldots, v_{n-1}$ with $v_1 + \cdots + v_{n-1} = du$. If one thinks of factoring p^{du} as $p^{v_1} \cdots p^{v_{n-1}}$, it is obvious that the number of non-negative $v_1, \ldots, v_{n-1}$ with $v_1 + \cdots + v_{n-1} = du$ is simply $d_{n-1}(p^{du})$. Thus, the number of possible anchors is $\binom{d}{n-1} d_{n-1}(p^{du})$, and the number of primitive solutions of $F(\mathbf{x}) = kp^u$ is not greater than

$$\binom{d}{n-1} d_{n-1}(p^{du}) M_{\mathfrak{C}}\ (k).$$

§7. Thue Equations with Few Coefficients.

Recall that the bound on the number of solutions to $F(x,y) = m$ depends only on d (the degree of F), and on m. Siegel (1929) hypothesized that there ought to be a bound for the number of solutions of certain diophantine equations $f(x,y) = 0$ which depends only on the number of non-zero coefficients.

We consider the special case of the Thue equations $F(x,y) = m$. For cubic Thue equations, the Siegel conjecture is incorrect. There is no bound independent of m. See Ch. IV, §8.

Consider the simplest Thue equation, namely the binomial one

$$ax^d - by^d = m, \qquad d \geq 3\ .$$

This equation had already been studied by Siegel, (1929) (1970), Domar (1954), Hyyrö (1964), Evertse (1982), and Mueller (1987). They achieved upper bounds $B = B(m)$ independent of the degree d. Consider also the trinomial Thue equation,

$$ax^d + bx^q y^{d-q} + cy^d = m, \qquad d \geq 3\ .$$

In this case, Mueller and Schmidt (1987) obtained a bound $B = B(m)$.

One may also study the more general Thue equations where F is a form of degree $d \geq 3$ with $s+1$ non-zero coefficients. That is, F may be written as

$$F(x,y) = \sum_{i=0}^{s} a_i x^{d_i} y^{d-d_i} \tag{7.1}$$

with $0 = d_0 < d_1 < \ldots < d_s = d$. It turned out to be just as easy to study the related "Thue inequality"

$$|F(x,y)| \leqq m\ . \tag{7.2}$$

Schmidt (1987) obtained a bound on the number of solutions, namely

$$\ll \sqrt{ds}\ m^{2/d}(1 + \log m^{1/d}).$$

Later, Mueller and Schmidt (1988) obtained a second bound, showing that the number of solutions of (7.2) is

$$\ll s^2\ m^{2/d}(1 + \log m^{1/d}).$$

This bound is itself bounded in terms of m and s, i.e. the number of coefficients of F, but independently of the degree. It is easily seen that the term $m^{2/d}$ is needed, but the logarithmic term is probably unnecessary. The term s^2 should probably be s.

In these Notes we will deal only with the binomial and trinomial case. We will prove (Mueller and Schmidt (1987)):

THEOREM 7A. *Suppose F is a binomial or trinomial of degree $d \geqq 9$. Then the number of solutions of the Thue Inequality (7.2) is*

$$\ll m^{2/d} .$$

If we combine this with Theorem 1C (to deal with $3 \leqq d \leqq 8$), we see that for any binomial or trinomial Thue inequality, the number of solutions is

$$\ll m^{2/d}(1 + \log m^{1/d}).$$

§8. The Distribution of the Roots of Sparse Polynomials.

By "sparse polynomial", we mean polynomials with few coefficients (as compared to their degree). Given a binary form

$$F(x,y) = \sum_{i=0}^{s} a_i x^{d_i} y^{d-d_i}$$

as in §7, we have a corresponding polynomial in one variable, $f(x)$, determined by $f(x) = F(x,1)$. That is,

$$f(x) = \sum_{i=0}^{s} a_i x^{di} \tag{8.1}$$

with $0 = d_0 < d_1 < \ldots < d_s$. In this section, we will study the distribution of the roots of such a sparse polynomial $f(x)$.

We start with the case $s = 2$, say

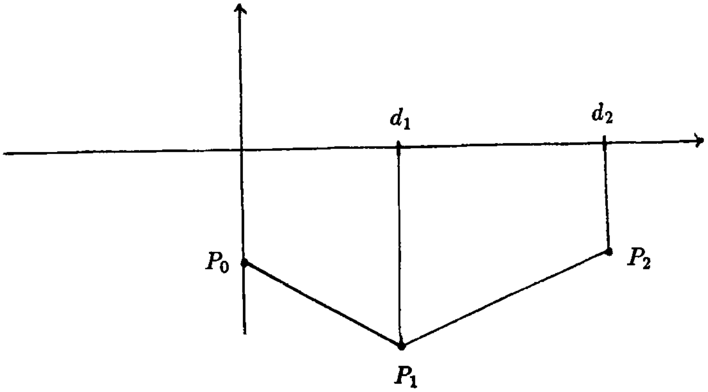
$$f(z) = a_0 + a_1 z^{d_1} + a_2 z^{d_2},$$

with $0 = d_0 < d_1 < d_2 = d$. First, suppose that a_1 is "large", i.e. $|a_1|$ is large relative to $|a_0|$, $|a_2|$. The polynomial $a_0 + a_1 z^{d_1}$ has d_1 roots, all of which satisfy $|z| = |a_0/a_1|^{1/d_1}$. Then it turns out that the original polynomial $f(z)$ has d_1 roots with $|z| \approx |a_0/a_1|^{1/d_1}$. Similarly, the polynomial $a_1 z^{d_1} + a_2 z^{d_2}$ has $d_2 - d_1$ nonzero roots satisfying $|z| = |a_1/a_2|^{1/(d_2-d_1)}$, and $f(z)$ has $d_2 - d_1$ roots with $|z| \approx |a_1/a_2|^{1/(d_2-d_1)}$. On the other hand, suppose that a_1 is "small" relative to a_0 and a_2. Then the polynomial $a_0 + a_2 z^{d_2}$ has d_2 roots with $|z| \approx |a_0/a_2|^{1/d_2}$. In this case, $f(z)$ has all $d_2 = d$ roots with $|z| \approx |a_0/a_2|^{1/d_2}$.

How may one remember this? Consider the three points

$$\begin{aligned} P_0 &= (0, -\log|a_0|), \\ P_1 &= (d_1, -\log|a_1|), \\ P_2 &= (d_2 - \log|a_2|). \end{aligned}$$

In the first case, when $|a_1|$ is large relative to $|a_0|$ and $|a_2|$, we have the following picture, with P_1 lying below the line segment $\overline{P_0P_2}$.



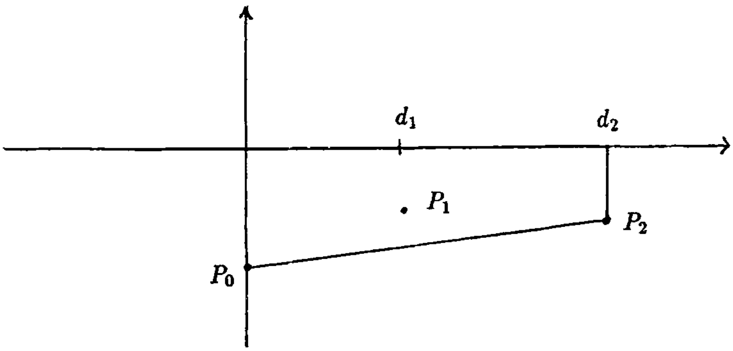
As discussed above, we have d_1 roots with

$$\log|z| \approx -\frac{\log|a_1| - \log|a_0|}{d} = \text{slope}\overline{P_0P_1},$$

and there are $d_2 - d_1$ roots with

$$\log|z| \approx -\frac{\log|a_2| - \log|a_1|}{d_2 - d_1} = \text{slope}\overline{P_1P_2}.$$

In the second case, when $|a_1|$ is small relative to $|a_0|$ and $|a_2|$, the point P_1 lies on or above the line segment $\overline{P_0P_2}$, as illustrated below.



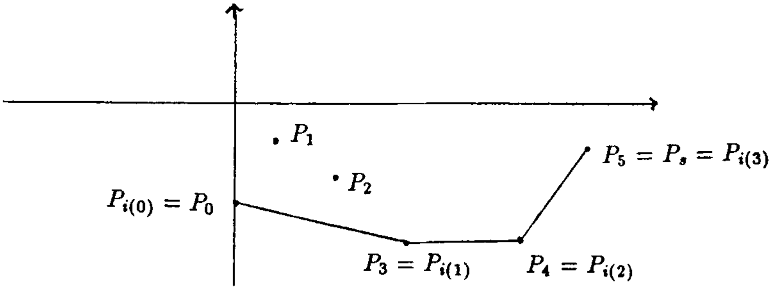
Here all $d = d_2$ roots satisfy

$$\log|z| \approx -\frac{\log|a_2| - \log|a_0|}{d_2} = \text{slope}\overline{P_0 P_2}.$$

Returning to the more general case, suppose we have a sparse polynomial f given by (8.1) with $0 = d_0 < d_1 < \ldots < d_s = d$. We call the points

$$P_i = (d_i, -\log|a_i|), \qquad (i = 0, \ldots, s),$$

the *Newton points.* The corresponding *Newton polygon* is defined to be the lower boundary of the convex hull of the Newton points. In other words, the polygon consists of points (x, y) in the convex hull such that $(x, y - \varepsilon)$ is not in the convex hull for $\varepsilon > 0$. For $s = 5$, we may have the following picture.



So that we may refer to each of the vertices of the Newton polygon, we label them $P_0 = P_{i(0)}, P_{i(1)}, \ldots, P_{i(\ell)} = P_s$, as shown above. For $1 \leqq u \leqq \ell$, we also let $\sigma(u)$ denote the slope of the line segment $\overline{P_{i(u-1)}\, P_{i(u)}}$. Since the Newton polygon is convex, $\sigma(u)$ is an increasing function of u.

By studying the case $s = 2$, we noticed that there is some relationship between the roots of the polynomial $f(z)$ and the Newton polygon of f. The following theorem illustrates this connection in the general case.

THEOREM 8A. *There exists a map from the set of roots of $f(z)$ to the set of segments of the Newton polygon such that exactly $d_{i(u)} - d_{i(u-1)}$ roots correspond to the segment $\overline{P_{i(u-1)}\, P_{i(u)}}$, and these roots have*

$$\Big|\log|z| - \sigma(u)\Big| < (2\log 3)s.$$

Remark. In p- adic analysis, the Newton polygon is well-known. In that case, $\log|z| = \sigma(u)$. See, e.g., Koblitz (1977), Ch. IV. The Theorem holds for all polynomials, sparse or not, but is probably more interesting in the sparse case.

Consider the circular ring (or annulus) R_u given by

$$e^{\sigma(u)-2\lambda s} < |z| < e^{\sigma(u)+2\lambda s},$$

where

$$\lambda = \log 3. \tag{8.2}$$

Then the theorem says that the $d_{i(u)} - d_{i(u-1)}$ roots are associated with an annulus R_u, and in fact, these roots lie in R_u. One should be aware, however, that there may be some overlapping of the annuli R_u. For this reason, we will call these annuli "large rings" and we will introduce another set of smaller annuli.

For $1 \leqq u \leqq \ell$, let S_u denote the "small ring" given by

$$e^{\sigma(u)-\lambda} < |z| < e^{\sigma(u)+\lambda}.$$

Two of these small annuli, say S_u and S_{u+1}, will overlap precisely if

$$\sigma(u+1) < \sigma(u) + 2\lambda.$$

In this case, the segments to the left and right of $P_{i(u)}$ have similar slopes, so the angle at the vertex $P_{i(u)}$ is not very sharp. We will say that the vertex $P_{i(u)}$ is "blunt". On the other hand, those vertices $P_{i(u)}$ with $\sigma(u+1) \geqq \sigma(u) + 2\lambda$ will be referred to as "sharp". By definition, we have that P_0 and P_s are sharp vertices. As with vertices in general, we would like a notation which allows us to refer to a particular sharp vertex. Suppose that we have sharp vertices $P_{i(u)}$ for $u(0) = 0,\ u(1), \ldots, u(p)\ell$. Setting $i[k] = i(u(k))$ for $k = 0, \ldots, p$, we have the sharp vertices $P_0 = P_{i[0]},\ P_{i[1]}, \ldots, P_{i[p]} = P_s$.

To eliminate the problem of overlap in the rings, we introduce a third set of annuli which we will call "medium rings". For $1 \leqq k \leqq p$, let L_k be the annulus given by

$$e^{\sigma(u(k-1)+1)-\lambda} < |z| < e^{\sigma(u(k))+\lambda}\ .$$

Then L_k is the union of the small annuli S_u with

$$u(k-1) + 1 \leqq u \leqq u(k). \tag{8.3}$$

The u in $u(k-1) < u < u(k)$ correspond to blunt vertices $P_{i(u)}$, so that

$$\sigma(u+1) \leqq \sigma(u) + 2\lambda \qquad \left(u(k-1) + 1 \leqq u < u(k)\right).$$

Thus, subsequent rings S_u, S_{u+1} in this range will overlap. Furthermore, by adding up the changes in the slopes of adjacent line segments, we have

$$\begin{aligned} \sigma(u(k)) &\leqq \sigma(u(k-1)+1) + 2\lambda(u(k) - u(k-1) - 1) \\ &\leqq \sigma(u(k-1)+1) + 2\lambda(s-1). \end{aligned}$$

Let L_k be any medium annulus and $z \in L_k$. For any u satisfying the corresponding inequality (8.3), we have

$$e^{\sigma(u)-2\lambda s} < |z| < e^{\sigma(u)+2\lambda s}$$

In other words, the medium ring L_k is contained in the intersection of the large rings R_u with u satisfying (8.3).

Using the medium annuli L_k, $(1 \leqq k \leqq p)$, we will see that it suffices to prove the following proposition in place of Theorem 8A.

PROPOSITION 8B. *Exactly $d_{i[k]} - d_{i[k-1]}$ roots lie in L_k $(1 \leqq k \leqq p)$.*

Theorem 8A does follow. We simply map the $d_{i[k]} - d_{i[k-1]}$ roots in L_k to the rings R_u with u satisfying (8.3), and we construct this mapping in such a way that $d_{i(u)} - d_{i(u-1}$ roots correspond to R_u. It is easily seen that Proposition 8B follows from the following

LEMMA 8C.

(i) *For $0 < k \leqq p$, precisely $d_{i[k]}$ roots lie in $|z| < e^{\sigma(u(k))+\lambda}$.*

(ii) *For $0 \leqq k < p$, precisely $d - d_{i[k]}$ roots lie in $|z| > e^{\sigma(u(k)+1)-\lambda}$.*

Proof. As before, let

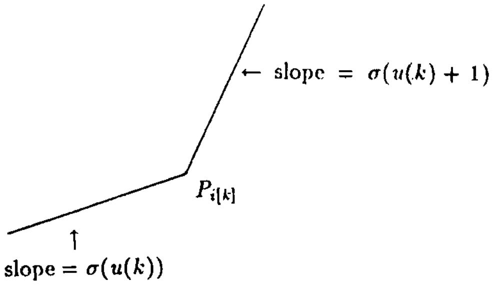
$$f(z) = \sum_{i=0}^{s} a_i z^{d_i} \ .$$

Given $\sigma \in R$, put $f^*(z) = f(e^\sigma z)$. Then the Newton points $P_{i(0)}, \dots, P_{i(\ell)}$ of f are mapped into the Newton points $P^*_{i(0)}, \dots, P^*_{i(\ell)}$ of f^* by the linear map $(x, y) \mapsto (x, y - \sigma x)$. In fact, the sharp vertices of f are mapped into the sharp vertices of f^*. This is easily seen by considering $\sigma^*(u)$, i.e. the slope of the segment to the left of $P^*_{i(u)}$ on the Newton polygon of f^*. We see that $\sigma^*(u) = \sigma(u) - \sigma$.

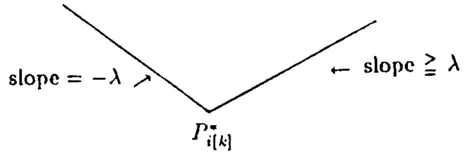
Given k corresponding to a sharp vertex $P_{i[k]}$, we put

$$\sigma = \sigma(u(k)) + \lambda \ .$$

Then $\sigma^*(u(k)) = \sigma(u(k)) - \sigma = -\lambda$ and $\sigma^*(u(k)+1) = \sigma(u(k)+1) - \sigma(u(k)) - \lambda \geqq 2\lambda - \lambda = \lambda$. We illustrate these facts in the following picture.



Newton polygon of f



Newton polygon of f^*

Then $P^*_{i[k]}$ is the "lowest" point on the Newton polygon of f^* for the chosen value of σ.

Now write

$$f^*(z) = \sum_{i=0}^{s} a_i^* z^{d_i} \ .$$

First, suppose that $i < i[k]$. Then the slope of the line segment $\overline{P_i^* P^*_{i[k]}}$ is $\leqq -\lambda$, since the Newton polygon is convex. Computing this slope, we get

$$-\ \frac{\log |a^*_{i[k]}| - \log |a_i^*|}{d_{i[k]} - d_i} \leqq -\lambda \ .$$

Thus

$$|a_i^*| \leqq |a^*_{i[k]}| e^{-\lambda(d_{i[k]}-d_i)} \ .$$

Since $\lambda = \log 3$, we have

$$|a_i^*| \leqq |a^*_{i[k]}| \ 3^{i-i[k]} \quad \text{for} \quad i < i[k].$$

In a similar way, one gets

$$|a_i^*| \leqq |a^*_{i[k]}| \ 3^{i[k]-i} \quad \text{for} \quad i > i[k].$$

What does this tell us when $k = p$? In that case, $i[k] = i[p] = s$ and we have

$$|a_i^*| \leqq |a_s^*| \ 3^{i-s} \quad \text{for} \quad i < s.$$

This will show that all of the roots of f^* lie in $|z| < 1$. To see this, suppose $|z| \geqq 1$. Then

$$\begin{aligned} |f^*(z)| &\geqq |z|^d \left(|a_s^*| \ - \ |a^*_{s-1}| - \ldots - \ |a_0^*|\right) \\ &\leqq |z|^d \ |a_s^*|(1 \ - \frac{1}{3} - \frac{1}{9} - \ldots) > 0. \end{aligned}$$

Since all of the roots of f^* lie in $|z| < 1$, we have that all the roots of f lie in $|z| < e^\sigma = e^{\sigma(u(p))+\lambda}$. Thus Lemma 8C (i) is true for $k = p$.

For $0 < k < p$, consider instead the polynomial

$$f_0(z) = \sum_{i=0}^{i[k]} \ a_i z^{d_i}$$

and the corresponding

$$f_0^*(z) = f_0(e^\sigma z) = \sum_{i=0}^{i[k]} \ a_i^* z^{d_i}$$

with σ given by (8.4). Applying our previous results to f_0, we know that all of the $d_{i[k]}$ roots of $f_0^*(z)$ lie in $|z| < 1$. We claim that exactly $d_{i[k]}$ roots of $f^*(z)$ are, in fact, in $|z| < 1$. Once this is proven, we will know that exactly $d_{i[k]}$ roots of $f(z)$ lie in $|z| < e^\sigma = e^{\sigma(u(k))+\lambda}$.

Using Rouché's Theorem to prove the claim, it will suffice to show that

$$|f_0^*(z) - f^*(z)| < |f_0^*(z)| \quad \text{for} \quad |z| = 1.$$

Then the polynomials f_0 and f_0^* will have the same number of roots in the disk $|z| < 1$. But for $|z| = 1$, we have

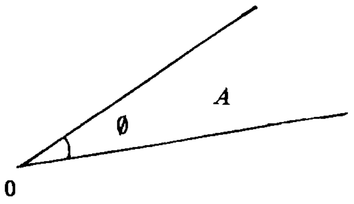
$$\begin{aligned} |f_0^*(z)| - |f_0^*(z) - f^*(z)| &\geqq |a^*_{i[k]}| - \sum_{i \neq i[k]} |a_i^*| \\ &> |a^*_{i[k]}| \left(1 - \frac{1}{3} - \frac{1}{9} - \ \ldots - \ \frac{1}{3} - \frac{1}{9} - \ \ldots\right) \\ &= 0. \end{aligned}$$

To prove part (ii), the lower bound for the zeros, put $\hat{f}(w) = w^d f(\frac{1}{w})$. Then the Newton polygon of $\hat{f}$ is obtained from the Newton polygon of f by a reflection through the line $x = d/2$. Under such a reflection, sharp vertices remain sharp and the bounds follow.

Exercise 8a. Let $f(z)$ be a polynomial with coefficients in a field E and $|\ |$ a non-Archimedean absolute value. Define the Newton polygon as before. Suppose that $f(z)$ has all of its roots in the field E. Then it is known (see, e.g., Koblitz (1977)) that one has a mapping from the roots to the segments of the Newton polygon such that roots corresponding to $\overline{P_{i(u-1)}\ P_{i(u)}}$ have $\log|z| = \sigma(u)$, where $\sigma(u)$ is the slope of this segment. Now prove this statement for a trinomial.

§9. The Angular Distribution of Roots.

In §8, we studied the radial distribution of the roots of a sparse polynomial $f(z)$. In this section, we will consider the angular distribution for binomials $f(z) = az^d + c$ and trinomials $f(z) = az^d + bz^q + c$. For a binomial, the roots make up a regular d-gon, so that the angular distribution is completely regular. In what follows, A will denote a wedge with vertex 0, i.e., a region bounded by two rays emanating from 0. Part or all of the boundary of A may belong to A. Write $|A| = \phi/2\pi$, where ϕ is the angle between the rays. We will consider the whole plane to be a wedge with $|A| = 1$.



With this notation, we have the following result, which also holds (trivially) for $b = 0$, i.e., for binomials.

THEOREM 9A. *Let $f(z)$ be a trinomial of degree d. If $Z(A)$ denotes the number of roots of f which lie in A, then*

$$\left| Z(A) - d|A| \right| \leqq 6 \; .$$

Proof. We may suppose that b is real since the roots of $f(z)$ are not affected when we multiply the polynomial by a suitable constant. Put $t = d - q$, so that $d = t + q$, and write the equation as $az^t + cz^{-q} = -b$. We may assume, without loss of generality, that $t \geqq q$ so that $t \geqq d/2$.

Introducing the notation $e(x) = e^{2\pi i x}$, write $a = |a|e(\alpha)$, $c = |c|e(\gamma)$, and $z = |z|e(\zeta)$. Then

$$|a| \; |z|^t \; e(t\zeta + \alpha) + |c| \; |z|^{-q} \; e(-q\zeta + \gamma) = -b \; .$$

The imaginary part of the left-hand side must be zero, so we have

$$|a| \; |z|^t \sin(2\pi(t\zeta + \alpha)) = |c| \; |z|^{-q} \sin(2\pi(q\zeta - \gamma)) \, .$$

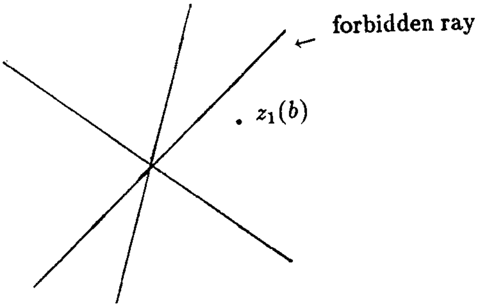
The left-hand side of this equality vanishes for some ζ_0, hence precisely for $\zeta_0 + (m/2t)$, for $m \in \mathbb{Z}$. The right-hand side may also vanish for one of these values. By a change of notations we can suppose that it vanishes at the same value ζ_0. In that case, the right-hand side will vanish at $\zeta_0 + (m'/2q)$ for $m' \in \mathbb{Z}$.

For the time being, we will require the additional hypothesis that $gcd(t, q) = 1$. Then $m/2t = m'/2q$ is possible only when $m/2t = m'/2q \in \frac{1}{2}\mathbb{Z}$. Thus, for the values

$$\zeta = \zeta_0 + (1/2t), \; \zeta_0 + (2/2t), \ldots, \zeta_0 + ((t-1)/2t), \; \zeta_0 + ((t+1)/2t), \ldots, \; \zeta_0 + ((2t-1)/2t),$$

the left-hand side vanishes but the right-hand side does not. If $\arg(z) = \zeta$ and ζ is one of the above values, then we see that z cannot be a root of f. The rays given by $\arg(z) = \zeta$, where ζ is one of the above, are called "forbidden rays" because they contain no solutions. Furthermore, these rays are determined independently of b.

Now let $a \neq 0$, $c \neq 0$ be fixed and denote the d roots of f as functions of b by $z_1(b), \ldots, z_d(b)$. One can arrange this such that the $z_i(b)$ are continuous functions of the real variable b. By the continuity of $z_i(b)$, we see that the values of $z_i(b)$ for various b can not cross any forbidden ray.



When $b = 0$, the roots of f form a regular d-gon and

$$\Big| Z(A) - d|A| \Big| \leqq 2.$$

Now let A be an angular domain bounded by two forbidden rays. We call such an A a "special angular domain". In that case, the continuity of the $z_i(b)$ gives

$$\Big| Z(A) - d|A| \Big| \leqq 2$$

for any b.

Now let A be an arbitrary angular domain. There exist special angular domains A_1, A_2 such that

$$A_1 \subset A \subset A_2$$

and

$$|A_2| - |A_1| \leqq 2/t \leqq 4/d\ .$$

(We do allow the possibility that A_1 is empty.) For the arbitrary angular domain A, we have

$$Z(A) \leqq Z(A_2) \leqq d|A_2| + 2 \leqq d|A| + d(|A_2| - |A_1|) + 2.$$

Then

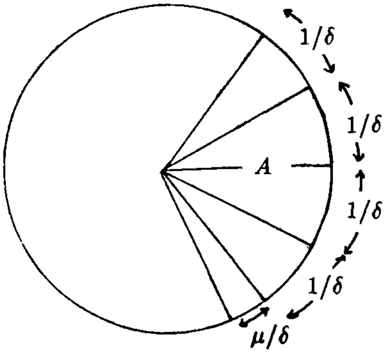
$$Z(A) \leqq d|A| + 6,$$

since $|A_2| - |A_1| \leqq 4/d$. The lower bound for $Z(A)$ is proved similarly.

Now we need only to remove the additional hypothesis that $gcd(t, q) = 1$. In general, we have $gcd(t, q) = \delta$. Write $d = \delta d_1$, $t = \delta t_1$, $q = \delta q_1$, so that $gcd(t_1, q_1) = 1$. The roots of f are of the type $z = w^{1/\delta}$ where w is a root of the polynomial $h(w) = aw^{d_1} + bw^{q_1} + c$. To each root w of h, there correspond δ roots of f which form a regular δ-gon. For any angular domain A, we have

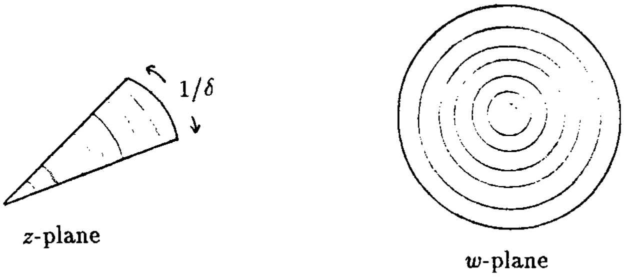
$$|A| = \frac{m}{\delta} + \frac{\mu}{\delta}\ ,$$

where $m \in \mathbb{Z}$ and $0 \leqq \mu < 1$, as illustrated.



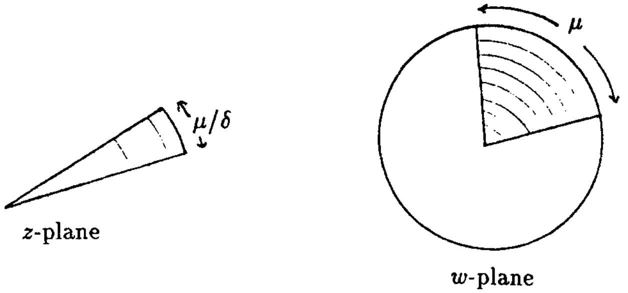
We will count the number of roots z of f in the domain A by considering the roots of h.

A domain of angle $1/\delta$ in the z-plane corresponds to a complete circle in the w-plane



Furthermore, every root w of h will give rise to a root z in each of the m domains of angle $1/\delta$. Thus we get $d_1 m$ roots in the portion of A of angle m/δ.

Now consider the portion of A of angle μ/δ in the z-plane. This corresponds to a angular domain B in the w-plane with $|B| = \mu$.



If Z' denotes the number of roots of h in the domain B, then

$$|Z' - d_1\mu| \leqq 6$$

by our previous work. Combining these results gives

$$\begin{aligned}\Big|Z(A) - d|A|\Big| &= \left|d_1 m + Z' - d\left(\frac{m}{\delta} + \frac{\mu}{\delta}\right)\right| \\ &= |d_1 m - d_1 m + Z' - d_1\mu| \\ &= |Z' - d_1\mu| \leqq 6.\end{aligned}$$

This result may be be generalized to a polynomial with an arbitrary number of terms, say

$$f(z) = \sum_{i=0}^{s} a_i z^{di} \ ,$$

as before. Khovansky (1981) showed in this case that

$$\left| Z(A) - d|A| \right| \leqq k(s)$$

where k depends only on s. Khovansky obtains $k(s)$ of the order of magnitude e^{cs^2}. This is almost certainly larger than need be. His work was related to an open question which we will discuss below. First, we consider a special case as an exercise.

Exercise 9a. Suppose $f(z)$ is a polynomial with $s+1$ terms as above. Show that f has not more than s positive, real roots.

Now suppose we have two polynomials $f(z,w)$, $g(z,w)$, each containing no more than $s+1$ monomials. Furthermore, suppose f and g have only finitely many (complex) zeros in common.

Conjecture. The polynomials f and g have not more than s^2 common real roots (z,w) in the first quadrant, i.e. $z > 0$, $w > 0$.

Khovansky showed that the number of such roots is not greater than $\ell(s)$, where $\ell(s)$ is some function similar to $k(s)$ above. The reader may find an account of Khovansky's work in Risler's (1984/85) paper.

Erdös and Turan (1950) gave another result on angular distribution. They considered polynomials of the form $f(z) = a_d z^d + \ldots + a_1 z + a_0$, where $a_0 \neq 0, a_d \neq 0$. In this case,

$$\left| Z(A) - d|A| \right| \leqq 16\left(d \log \frac{|a_0| + |a_1| + \ldots + |a_d|}{|a_0 a_d|^{1/2}} \right)^{1/2} .$$

If all the coefficients are close in absolute value, then we have the bound $\ll (d \log d)^{1/2}$.

We now return to trinomials.

THEOREM 9B. *Let $f(z)$ be a trinomial of degree d with roots $\alpha_1, \ldots, \alpha_d$. Then there is a subset of these roots, say $\delta_1, \ldots, \delta_\ell$, where $\ell \leqq 32$, such that for every real ζ, we have*

$$\min_{1 \leqq j \leqq \ell} |\zeta - \delta_j| \leqq e^{10} d \min_{1 \leqq i \leqq d} |\zeta - \alpha_i| .$$

Remark. The numbers 32 and e^{10} are larger than need be. A similar result holds for polynomials with $s+1$ terms, where 32 and e^{10} are replaced by constants which depend on s. See Schmidt (1987).

Proof. In the case of a trinomial, the corresponding Newton polygon has either one or two segments. Hence the roots of a trinomial lie in one or two annuli of the type

$$\left| \log |z| - \sigma \right| \leqq (2\lambda)(2) = 4\lambda < 5 .$$

Thus

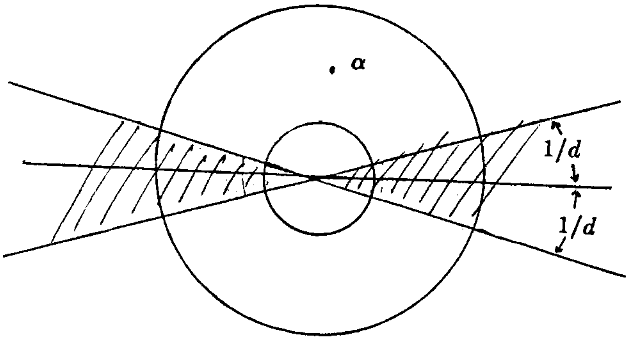
$$e^{\sigma - 5} < |z| < e^{\sigma + 5},$$

which we will write as

$$B_1 < |z| < B_2,$$

where $B_2/B_1 = e^{10}$.

Consider the following picture.



The number of roots in each of these two angular domains is not greater than $d|A|+6 = 8$, since $|A| = 2/d$. So, there are at most 16 roots in the two angular domains together. Now suppose that α is a root in the annulus which is not in one of these angular domains. Suppose δ is any root in the annulus. Let $\zeta \in R$. If $|\zeta| \geqq 2B_2$, then $|\zeta - \alpha| \geqq B_2$ and

$$\begin{aligned} |\zeta - \delta| &\geqq |\zeta - \alpha| + |\alpha - \delta| \\ &\leqq |\zeta - \alpha| + 2B_2 \\ &\leqq 3\ |\zeta - \alpha| < e^{10} d\ |\zeta - \alpha|. \end{aligned}$$

On the other hand, if $|\zeta| < 2B_2$, then write $\alpha = \rho e(\eta)$, where $|\eta| \leqq 1/2$. First, say $|\eta| \leqq 1/4$. Then $|\eta| \geqq 1/d$ since α is not in the angular domains. We have

$$|\zeta - \delta| \leqq |\zeta| + |\delta| < 3B_2.$$

In this case, we also have

$$|\zeta - \alpha| \geqq |\mathfrak{I}m\alpha| = |\rho\sin(2\pi\eta)| \geqq 4\rho\eta \geqq 4B_1/d.$$

Combining these two estimates, gives

$$|\zeta - \delta| \leqq \frac{3}{4}\ d\ \frac{B_2}{B_1}\ |\zeta - \alpha| < e^{10} d\ |\zeta - \alpha|.$$

It is now clear that the theorem holds with $\delta_1, \ldots, \delta_\ell$ the roots in the angular domains in each of the annuli, if there are such roots. If the angular domains in one of the annuli contains no root, but if there are roots in this annulus, then we pick one such root to be among $\delta_1, \ldots, \delta_\ell$. Clearly, the Theorem holds with this choice.

§10. On Trinomials.

Initially, we will consider trinomials of the form $g(z) = z^d + \mu z^q \pm 1$. We will write $M = |\mu|$ and $d = q + t$.

LEMMA 10A.
(i) *When $M \geqq 3^{4d}$, then g has exactly t roots in the annulus*

$$M^{1/t}\, 3^{-4} < |z| < M^{1/t}\, 3^4 ,$$

and exactly q roots in

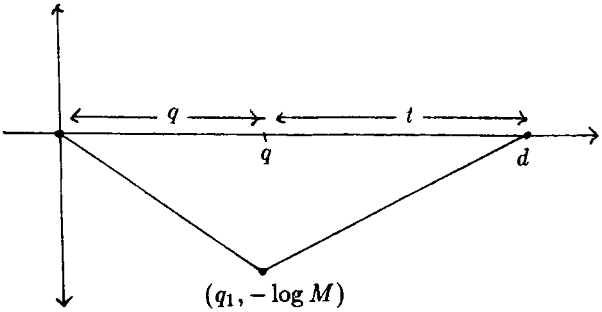
$$M^{1/q}\, 3^{-4} < |z|^{-1} < M^{1/q}\, 3^4 .$$

(ii) *When $M < 3^{4d}$, then all d roots of g lie in the annulus*

$$3^{-4(d+1)} < |z| < 3^{4(d+1)} .$$

Remark. In case (i), roots z in the first annulus have $|z| > 1$ and those in the second annulus have $|z| < 1$. In what follows, we will call these "large" roots and "small" roots, respectively.

Proof. Consider the Newton polygon for $g(z)$, illustrated below.



When $M > 1$, the Newton polygon has two segments, and when $M \leqq 1$ it has only one.

In case (i), apply Theorem 8A to see that there are t roots corresponding to the second segment with

$$\left| \log|z| - \frac{\log M}{t} \right| \leqq 4 \log 3 .$$

So we have

$$M^{1/t}\, 3^{-4} < |z| < M^{1/t}\, 3^4 .$$

Similarly, there are q roots corresponding to the first segment which satisfy

$$\left| \log|z| + \frac{\log M}{q} \right| \leqq 4 \log 3.$$

Then

$$M^{-1/q}\, 3^{-4} < |z| < M^{-1/q}\, 3^4 .$$

In case (ii), since $M < 3^{4d}$, we may have either one or two segments on the Newtwon polygon, as mentioned above. The absolute value of the slope of any segment, however, is not greater than $\log M < (4\log 3)d$. Using Theorem 8A once again, we know that all roots have

$$-(d+1)(4\log 3) < \log|z| < (d+1)(4\log 3).$$

That is, all d roots satisfy

$$3^{-4(d+1)} < |z| < 3^{4(d+1)} .$$

We introduce the notation $A \succ B$ to mean that $A \geqq B/K^d$, where K is an absolute constant.

LEMMA 10B.

(i) *When $M \geqq 3^{4d}$, then every large root z has*

$$|g'(z)| \succ M^{(d-1)/t}$$

and every small root z has

$$|g'(z)| \succ M^{1/q} .$$

(ii) *When $M < 3^{4d}$, then every root has either*

$$|g'(z)| \succ 1 \qquad \text{or} \qquad |g''(z)| \succ 1 .$$

Proof. (i). Since $g(z) = z^d + \mu z^q \pm 1$, we have $g'(z) = dz^{d-1} + q\mu z^{q-1} = dz^{d-1} + d\mu z^{q-1} - t\mu z^{q-1} \pm \frac{d}{z} \mp \frac{d}{z}$. If z is a root, then

$$dz^{d-1} + d\mu z^{q-1} \pm \frac{d}{z} = \frac{dg(z)}{z} = 0,$$

and we have

$$\begin{aligned} |g'(z)| &= \left| - t\mu z^{q-1} \mp \frac{d}{z} \right| \\ &\geqq \frac{1}{|z|} \ (tM|z|^q - d) \ . \end{aligned}$$

If z is a large root of g, then $M^{1/t}\, 3^{-4} < |z|$, so that

$$|g'(z)| \geqq \frac{1}{M^{1/t}\, 3^4} \left(tM^{1+(q/t)}3^{-4q} - d\right) .$$

Furthermore, $tM^{1+(q/t)}\, 3^{-4q} \geqq M > 2d$, so that we have

$$\begin{aligned} |g'(z)| &\geqq \frac{M^{1+(q/t)}}{2 \cdot 3^4 \cdot 3^{4d} \cdot M^{1/t}} \\ &\succ M^{(d-1)/t} . \end{aligned}$$

If z is a small root of g, then $\hat{z} = 1/z$ is a large root of the reciprocal polynomial $\hat{g}(z) = \pm z^d + \mu z^t + 1$. In that case, $|\hat{z}| \leqq M^{1/q}\, 3^4$ and $|\hat{g}'(\hat{z})| \succ M^{(d-1)/q}$. The original polynomial $g(z)$ and its reciprocal polynomial $\hat{g}(z)$ are related by the equation

$g(z) = z^d\ \hat{g}(\frac{1}{z})$. From the product rule and the fact that $\hat{g}(\hat{z}) = 0$ for a root z of g, we get

$$g'(z) = -z^{d-2}\ \hat{g}'(\hat{z}) = -\hat{z}^{2-d}\hat{g}'(\hat{z}) .$$

Then

$$|g'(z)| \succ M^{(2-d)/q}\ M^{(d-1)/q} = M^{1/q} .$$

Now we look at case (ii). From the first part of the proof, we have

$$g'(z) = -t\mu z^{q-1} \mp \frac{d}{z}$$

when z is a root of g. Starting with the original polynomial g and differentiating twice, we get

$$\begin{aligned} g''(z) &= d(d-1)z^{d-2} + \mu q(q-1)z^{q-2} \\ &= d(d-1)\ \frac{g(z)}{z^2} + \mu(q(q-1) - d(d-1))z^{q-2} \mp \frac{d(d-1)}{z^2} \cdot \end{aligned}$$

As previously, the first term vanishes if z is a root. In that case,

$$g''(z) = \mu(q(q-1) - d(d-1))z^{q-2} \mp \frac{d(d-1)}{z^2} .$$

Now consider the expression

$$zg'(z)(d(d-1) - q(q-1)) - z^2g''(z)t = \mp d(d(d-1) - q(q-1) - t(d-1)) = \mp dqt .$$

This equation implies that either

$$|zg'(z)(d(d-1) - q(q-1))| \geqq dqt/2$$

or

$$|z^2g''(z)t| \geqq dqt/2 .$$

In other words, either

$$|zg'(z)| \succ 1 \qquad \text{or} \qquad |z^2g''(z)| \succ 1 .$$

By Lemma 10A, we have $|z| \prec 1$, so that

$$|g'(z)| \succ 1 \quad \text{or} \quad |g''(z)| \succ 1.$$

The two preceding lemmas dealt with trinomials of the form $g(z) = z^d + \mu z^q \pm 1$. In general, we have $f(z) = az^d + bz^q \pm c \in \mathbb{Z}[z]$, where $a, c > 0$. Put

$$\mu = ba^{-q/d}\ c^{-t/d} \quad \text{and} \quad M = |\mu| .$$

Then $f(z) = cg(w)$, where $w = (a/c)^{1/d}z$. Now the various cases will depend on $H = \max\ (a,\ |b|,\ c)$. We will suppose that $a,\ b,\ c$ are integers, so that in particular $a \geqq 1,\ c \geqq 1$.

LEMMA 10C. *If $M \geqq 3^{4d}$ and $H = c$, then every root of f has*

$$|f'(z)| \succ H^{1-(1/d)} .$$

Proof. As we have seen, $f(z) = cg((a/c)^{1/d}z)$, so

$$|f'(z)| = c(a/c)^{1/d}\ |g'((a/c)^{1/d}z)| .$$

If z is a root of f, then $(a/c)^{1/d}z$ is a root of the special polynomial g, and by Lemma 10B, we know that $|g'((a/c)^{1/d}z)| \succ 1$. Therefore,

$$|f'(z)| \succ c(a/c)^{1/d} = a^{1/d}c^{1-(1/d)} \geqq H^{1-(1/d)},$$

since $a \geqq 1$.

LEMMA 10D. *If $M \geqq 3^{4d}$ and $H = |b|$, then every large root of f has*

$$|f'(z)| \succ P^q\ H^{1-(2/d)} ,$$

where

$$P = \left(\frac{|b|}{a}\right)^{(1-1/d)/t} \left(\frac{|b|}{c}\right)^{(1/d)/q} .$$

Proof. As before, we have $f(z) = cg((a/c)^{1/d}z)$ and

$$\begin{aligned} |f'(z)| &= c(a/c)^{1/d}\ |g'((a/c)^{1/d}z)| \\ &\succ c(a/c)^{1/d}\ M^{(d-1)/t} \\ &= \left(\frac{|b|^{d-1}}{a^{q-1}}\right)^{1/t} = \dots \\ &= P^q a^{1/d}\ |b|^{1-(2/d)}\ c^{1/d} \\ &\geqq P^q\ H^{1-(2/d)} . \end{aligned}$$

LEMMA 10E. *Suppose $M < 3^{4d}$ and $a \leqq c$. Then every root of f has either*

$$|f'(z)| \succ H^{1-(1/d)} \qquad \text{or} \qquad |f''(z)| \succ H^{1-(2/d)} .$$

Proof. Since $M \prec 1$, we have $|b| \prec a^{q/d}\ c^{t/d} \prec c$ and $H \prec c$. From the chain rule, with $w = (a/c)^{1/d}z$,

$$|f'(z)| = a^{1/d}\ c^{1-(1/d)}\ |g'(w)|$$

and

$$|f''(z)| = a^{2/d}\ c^{1-(2/d)}\ |g''(w)|.$$

By Lemma 10B, either

$$|f'(z)| \succ a^{1/d}\ c^{1-(1/d)} \succ H^{1-(1/d)}$$

or

$$|f''(z)| \succ a^{2/d}\, c^{1-(2/d)} \succ H^{1-(2/d)}.$$

§11. Roots of f close to $\frac{x}{y}$.

We now return to the Thue inequality

$$|F(x,y)| \leqq m, \tag{11.1}$$

where F is the homogeneous polynomial given by

$$F(X,Y) = aX^d + bX^qY^t \pm cY^d\ ,$$

with a, $c > 0$. We will see that either there exists a root α of $f(z) = F(z,1)$ which is close to $\frac{x}{y}$, or there exists a root β of the reciprocal polynomial $\hat{f}(z) = F(1,z)$ which is close to $\frac{y}{x}$. We must distinguish several cases.

LEMMA 11A. *Let $H = \max(a,c)$. Suppose that $M \geqq 3^{4d}$ and (x,y) is a solution to (11.1) with $x \neq 0$, $y \neq 0$. Then either there is a root α of $f(z) = F(z,1)$ with*

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{mH^{(1/d)-1}}{|y|^d}\ ,$$

or there is a root β of $\hat{f}(z) = F(1,z)$ with

$$\left|\beta - \frac{y}{x}\right| \prec \frac{mH^{(1/d)-1}}{|x|^d}\ .$$

Proof. We may suppose that $H = c$. In this case, we will see that the first alternative holds. By Lemma 3A, with the parameter $u = 1$, there is a root α of f with

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{m}{|f'(\alpha)|\ |y|^d}\ .$$

Furthermore, by Lemma 10C, we have $|f'(\alpha)| \succ H^{1-(1/d)}$, so that

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{mH^{(1/d)-1}}{|y|^d}\ .$$

The second case follows similarly when $H = a$.

LEMMA 11B. *Suppose $M \geqq 3^{4d}$ and $H = |b|$, and (x,y) is a solution to (11.1) with $x \neq 0$, $y \neq 0$. Then either there is a large root α of $f(z) = F(z,1)$ with*

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{mH^{(2/d)-1}}{|y|^d}\ ,$$

or there is a large root β of $\hat{f}(z) = F(1, z)$ with

$$\left|\beta - \frac{y}{x}\right| \prec \frac{mH^{(2/d)-1}}{|x|^d} .$$

Proof. The polynomial $f(z)$ has t large roots, say $\alpha_1, \ldots, \alpha_t$, and q small roots, say $1/\beta_1, \ldots, 1/\beta_q$. Then the reciprocal polynomial $\hat{f}$ has large roots $\beta_1, \ldots, \beta_q$ and small roots $1/\alpha_1, \ldots, 1/\alpha_t$. Let

$$L = \min\left(|x - \alpha_1 y|, \ldots, |x - \alpha_t y|\right)$$

and

$$\hat{L} = \min\left(|y - \beta_1 x|, \ldots, |y - \beta_q x|\right),$$

and consider the two real numbers

$$L\left(\frac{a}{|b|}\right)^{(1-1/d)/t}, \qquad \hat{L}\left(\frac{c}{|b|}\right)^{(1-1/d)/q} .$$

By symmetry, we may suppose that

$$L\left(\frac{a}{|b|}\right)^{(1-1/d)/t} \leqq \hat{L}\left(\frac{c}{|b|}\right)^{(1-1/d)/q} .$$

We will see that the first case follows.

We have

$$\hat{L} \leqq |y - \beta_k x| = |\beta_k|\,|x - \beta_k^{-1}\, y| \qquad (1 \leqq k \leqq q),$$

so that

$$L \leqq \left(\left(\frac{|b|}{a}\right)^{1/t}\left(\frac{c}{|b|}\right)^{1/q}\right)^{1-(1/d)} |\beta_k|\,|x - \beta_k^{-1}\, y| \qquad (1 \leqq k \leqq q).$$

Now β_k is a large root of $\hat{f}$, so β_k is $(a/c)^{1/d}$ times a large root of $\hat{g}$. Then we have

$$|\beta_k| \prec (a/c)^{1/d}\, M^{1/q} = (|b|/c)^{1/q}$$

and

$$L \prec \left(\frac{|b|}{a}\right)^{(1-1/d)/t}\left(\frac{|b|}{c}\right)^{1/qd} |x - \beta_k^{-1} y| = P\,|x - \beta_k^{-1} y| \qquad (1 \leqq k \leqq q),$$

where P is as in Lemma 10D.

By reordering, we may suppose that $L = |x - \alpha_1\, y|$. Then

$$|(\alpha_1 - \alpha_j)y| \leqq |x - \alpha_1 y| + |x - \alpha_j y| \leqq 2\,|x - \alpha_j y| \qquad (2 \leqq j \leqq t).$$

From our work above, we also have

$$\begin{aligned}\left|\left(\alpha_1 - \frac{1}{\beta_k}\right) y\right| &\leqq |x - \alpha_1 y| + |x - \beta_k^{-1} y| \\ &\prec P|x - \beta_k^{-1} y| + |x - \beta_k^{-1} y| \\ &\prec P|x - \beta_k^{-1} y|, \qquad (1 \leqq k \leqq q)\end{aligned}$$

since $P \geqq 1$. Writing f as a product of its linear factors, differentiating, evaluating at $x = \alpha_1$, and multiplying by $|x - \alpha_1 y|\ |y^{d-1}|$ gives

$$\begin{aligned}|x - \alpha_1 y|\ |f'(\alpha_1) y^{d-1}| &= |x - \alpha_1 y|\ a \prod_{2 \leqq j \leqq t} |\alpha_1 - \alpha_j) y| \prod_{1 \leqq k \leqq q} \left|\left(\alpha_1 - \frac{1}{\beta_k}\right) y\right| \\ &\prec P^q a \prod_{1 \leqq j \leqq t} |x - \alpha_j y| \prod_{1 \leqq k \leqq q} |x - \beta_k^{-1} y|.\end{aligned}$$

But $|F(x,y)| = a \prod_{1 \leqq j \leqq t} |x - \alpha_j y| \prod_{1 \leqq k \leqq q} |x - \beta_k^{-1} y|$, so that by (11.1) we have

$$\left|\alpha_1 - \frac{x}{y}\right| \prec \frac{mP^q}{|f'(\alpha_1)|\ |y|^d} .$$

Furthermore, Lemma 10D gives a lower bound for the derivative, namely

$$|f'(\alpha_1)| \succ P^q H^{1-(2/d)} .$$

Then

$$\left|\alpha_1 - \frac{x}{y}\right| \prec \frac{mH^{(2/d)-1}}{|y|^d} ,$$

as desired.

LEMMA 11C. *Suppose $M < 3^{4d}$, and (x,y) is a solution to (11.1) with $x \neq 0$, $y \neq 0$. If $a \leqq c$, then there is a root α of f satisfying either*

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{m\ H^{(1/d)-1}}{|y|^d} , \tag{11.2}$$

or

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{m^{1/2}\ H^{(1/d)-(1/2)}}{|y|^{d/2}} . \tag{11.3}$$

If $c \leqq a$, then there is a root β of $\hat{f}$ with either

$$\left|\beta - \frac{y}{x}\right| \prec \frac{mH^{(1/d)-1}}{|x|^d} ,$$

or

$$\left|\beta - \frac{y}{x}\right| \prec \frac{m^{1/2} H^{(1/d)-(1/2)}}{|x|^{d/2}} .$$

Proof. By symmetry, we may assume $a \leqq c$. Once again, apply Lemma 3A, this time with $u = 1$ and $u = 2$. We see that there is a root α of f with

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{m}{|f'(\alpha)|\ |y|^d}$$

and with

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{m^{1/2}}{|f''(\alpha)|^{1/2}\ |y|^{d/2}} .$$

By Lemma 10E, either $|f'(\alpha)| \succ H^{1-(1/d)}$ or $|f''(\alpha)| \succ H^{1-(2/d)}$, which gives the two cases above, respectively.

In the next section, we will complete the proof of Theorem 7A, which gives a bound on the number of solutions of the Thue inequality (11.1). For any solution pair (x, y), there may be a different α satisfying one of the results in this section. This could possibly introduce a factor of d. However, Theorem 9B allows us to restrict ourselves to as few as 32 roots α if we are willing to give up a factor which is $\prec 1$. So it remains for us to estimate the number of integers (x, y) satisfying one of the lemmas in this section for a fixed root α.

Before doing so, we would like to combine our lemmas to get a single relation. Write

$$K = mH^{(2/d)-1} \tag{11.4}$$

Then (11.3) in Lemma 11C becomes

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{K^{1/2}}{|y|^{d/2}}$$

and all of the other relations for α imply

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{K}{|y|^d}.$$

If we restrict ourselves to solutions where $\min(|x|,\ |y|) \geqq K^{1/d}$, then we see that it will suffice to study

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{K^{1/2}}{|y|^{d/2}} .$$

By symmetry, a similar result holds for roots $1/\beta$.

§12. Proof of Theorem 7A.

Recall, in Theorem 7A, we give a bound on the number of solutions of

$$|F(x, y)| \leqq m ,$$

where $F(x, y)$ is an irreducible trinomial of degree $d \geqq 9$. As in the previous sections, we write

$$F(x, y) = ax^d + bx^t y^{d-t} \pm cy^d ,$$

with $a > 0,\ c > 0$. We let $h = \max(a, |b|,\ c)$ and $K = m/h^{1-(2/d)}$.

THEOREM 12A.

(a) *If F is a trinomial with $d \geqq 9$ and $K \leqq 1$, then the number of primitive solutions of the Thue inequality above is*

$$\ll 1 + \frac{\log^+(\log m/\log(2/K))}{\log d} \ll 1 + \frac{\log^+ \log m}{\log d} .$$

(b) *If F and d are as above and $K > 1$, then the number of primitive solutions to the Thue inequality with*

$$\min(|x|,\ |y|) > c_1\ K^{1/(d-4)}$$

is

$$\ll 1 + \frac{\log^+ \log m}{\log d} .$$

COROLLARY 12B. *If $m \leqq H^{1-(3/d)}$, then the number of solutions is $\ll 1$.*

The corollary follows since $m \leqq H^{1-(3/d)}$ gives $1/K \geqq H^{1/d}$. Then

$$\log m/\log(2/K) \ll (\log H)/(\frac{1}{d}\log H) = d .$$

Remark. In fact, the corollary is still true when the 3 is replaced by any constant greater than 2.

Proof (Theorem 12A). Let $\alpha_1, \dots, \alpha_d$ be the roots of $f(z) = F(z,1)$. By Lemma 7B of Chapter I, $h(\alpha_1)\dots h(\alpha_d) \leqq 5^{d/2}\ H(f) \prec H$. In particular, each root α has $h(\alpha) \prec H$. Since $d \geqq 9$, we have

$$\frac{d/2}{\sqrt{2d}} = \sqrt{\frac{d}{8}} \leqq \sqrt{\frac{9}{8}} = \chi^2 > 1 ,$$

with $\chi = \sqrt[4]{9/8}$.

In case (a), in view of what we said at the end of the last section, we need to consider

$$\left|\alpha - \frac{x}{y}\right| \prec \frac{K^{1/2}}{y^{d/2}} .$$

That is, look at

$$\left|\alpha - \frac{x}{y}\right| < \frac{c_2^d\ K^{1/2}}{y^{d/2}} < \frac{K^{1/2}}{4\ y^{d/2\chi}} < \frac{1}{y^{d/2\chi}} \tag{12.1}$$

if $y > c_3$. The exponent in the last inequality is $\mu = d/2\chi \geqq \chi\sqrt{2d}$. Thus, by Theorem 9A of Chapter II, the number of solutions with $|y| \geqq h(\alpha)$ is $\ll 1$.

Next consider solutions of (12.1) with $c_3 \leqq |y| \leqq h(\alpha)$. Suppose these solutions have denominators $c_3 \leqq y_0 \leqq y_1 \leqq \cdots \leqq y_\nu \leqq h(\alpha)$. By the Gap Principle, we have

$$y_{j+1} \geqq \frac{2}{K^{1/2}} y_j^{(d/2\chi)-1} \geqq \frac{2}{K^{1/2}} y_j^{d/3} ,$$

and so

$$h(\alpha) \geqq y_\nu \geqq \left(\frac{2}{K^{1/2}}\right)^{(d/3)\nu-1} .$$

This gives a bound on the number of denominators, namely

$$\nu + 1 \leqq 2 + \frac{\log^+(\log h(\alpha)/\log\,(2/K^{1/2}))}{\log\,(d/3)} .$$

Since $h(\alpha) \prec H$, (i.e. $h(\alpha) \leqq c_4^d H$), we have

$$\nu + 1 \ll 2 + \frac{\log^+(\log H/\log\,(2/K^{1/2}))}{\log d} .$$

Furthermore,

$$\begin{aligned} \log H/\log(2/K^{1/2}) &\ll (\log m + \log(1/K))/\log(2/K^{1/2}) \\ &\ll 1 + (\log m/\log(2/K)) , \end{aligned}$$

and we see that the number of solutions in this case is

$$\ll 1 + \frac{\log^+\,(\log m/\log(2/K))}{\log d} .$$

For part (a) of the theorem, it remains to count the solutions with $|y| \leqq c_3$. This will be done after stating Lemma 12C, which follows shortly.

In part (b), we have $K > 1$. As before, we consider the inequality

$$\left|\alpha - \frac{x}{y}\right| < \frac{c_2^d\,K^{1/2}}{y^{d/2}} < \frac{c_2^d\,K^{1/2}}{y^{\chi\sqrt{2d}}\,y^{c_5 d}} . \tag{12.2}$$

If $y > c_6\,K^{c_7/d}$, then

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{\chi\sqrt{2d}}} .$$

Again by Theorem 9A of Chapter II, the number of solutions with $y \geqq h(\alpha)$ is $\ll 1$. Thus it remains to count the solutions with $y \leqq \max\,(c_6 K^{c_7/d},\ h(\alpha))$.

We rewrite the inequality in (12.2) as

$$\left|\alpha - \frac{x}{y}\right| < \frac{c_2^d\,K^{1/2}}{y^{d/2}} = \frac{A}{y^{d/2}} = \frac{A}{y^{2+\delta}} , \tag{12.3}$$

where $\delta = (d/2) - 2$. By a variation of Lemma 8C of Chapter II, we know that the number of solutions to (12.3) with $W \leqq y < W^C$, where $W \geqq (4A)^{1/\delta}$, is

$$\ll 1 + \frac{\log (C \log W)}{\log(1+\delta)} .$$

In our particular case, we want to count solutions with

$$(4A)^{1/\delta} \leqq y \leqq \max (c_6 K^{c_7/d},\ h(\alpha)),$$

so we let $W = (4A)^{1/\delta}$ and

$$C = \frac{\log c_6 K^{c_7/d}}{\log(4A)^{1/\delta}} \quad \text{or} \quad C = \frac{\log h(\alpha)}{\log (4A)^{1/\delta}} .$$

In the first case, in view of $A = c_2^d\ K^{1/2}$, we have $C \ll 1$, and in the second, $C \leqq \log h(\alpha) \leqq \log (c_4^d H) \ll d + \log m$. We also have

$$\log W = \log (4A)^{1/\delta} \ll 1 + \log m ,$$

and the bound on the number of solutions becomes

$$\ll 1 + \frac{\log^+ \log m}{\log d} .$$

In case (b), we are left with solutions with $|y| < (4A)^{1/\delta} \leqq c_7 K^{1/2\delta} = c_7 K^{1/(d-4)}$. Thus by the way Theorem 12A (b) was formulated, we are finished with this case. In case (a), it remains to count solutions with $|y| \leqq c_3$. We will finish this after the following lemma.

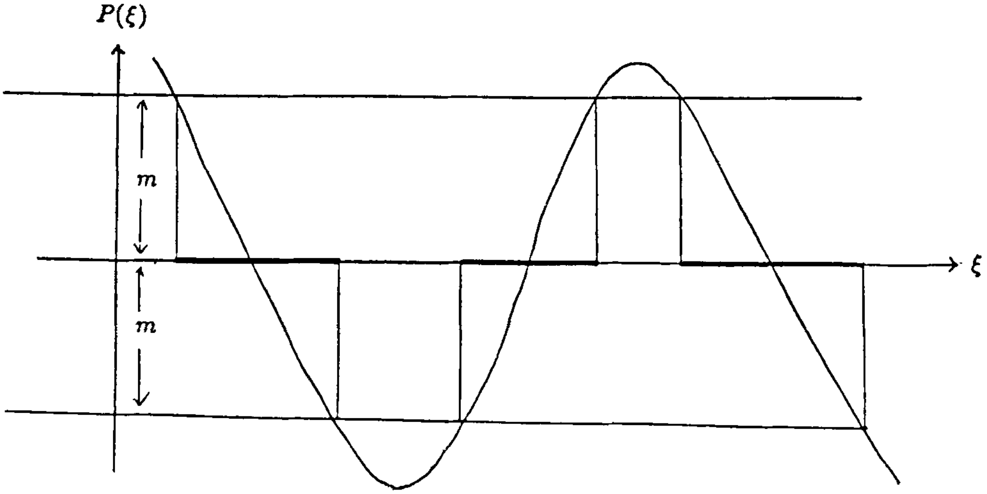
LEMMA 12C. *Let $p(X) = AX^d + BX^q + C$ be a polynomial. The real numbers ξ with*

$$|p(\xi)| \leqq m$$

fall into the union of at most eight intervals of total length

$$\ll 1 + \left(\frac{m}{|A|}\right)^{1/d} \min \left(1, \left(\frac{m}{|B|}\right)^{(1/2)-(1/d)}, \left(\frac{m}{|C|}\right)^{(1/2)-(1/d)}\right).$$

The proof will not be given here, but the following picture may give the reader some indication as to what goes on.



For a proof (using only calculus) see Mueller and Schmidt (1987, Lemma 7.1). In particular, if $|A| \geqq 1$, the total length is

$$\ll 1 + \min\left(\left(\frac{m}{|A|}\right)^{1/d}, \frac{m^{1/2}}{|B|^{(1/2)-(1/d)}}, \frac{m^{1/2}}{|C|^{(1/2)-(1/d)}}\right).$$

Now we are able to complete the proof of part (a) of Theorem 12C. Recall that we left open the number of solutions of $|F(x,y)| \leqq m$ where $|y| \leqq c_3$ (or when $|x| \leqq c_3$). For given y, consider the polynomial

$$\begin{aligned} p(X) = F(X,y) &= aX^d + by^t\, X^q + cy^d \\ &= AX^d + BX^q + C\ , \end{aligned}$$

with $A = a$, $B = by^t$, $C = \pm cy^d$. We have $K \leqq 1$, so that $m \leqq H^{1-(2/d)}$, and then $m^{1/2} \leqq H^{(1/2)-(1/d)}$. For each $y \neq 0$, the lemma tells us that the number of solutions is $\ll 1$. When $y = 0$, the only possible primitive points are $(1,0)$ and $(-1,\ 0)$. All together, we have $\ll 1$ solutions in this case.

We may now prove the main theorem, which we state again for the reader.

THEOREM 7A. *If $F(X,Y)$ is an irreducible trinomial of degree $d \geqq 9$, then the number of solutions of*

$$|F(x,y)| \leqq m$$

is

$$\ll m^{2/d}\ .$$

Proof. As in section 2, it suffices to show that

$$P(m) \ll m^{2/d} ,$$

where $P(m)$ denotes the number of primitive solutions. By Theorem 12A, we have

$$P(m) \ll 1 + \frac{\log^{+} \log m}{\log d} ,$$

provided that $K \leqq 1$ or $\min(|x|,\ |y|) \geqq c_1\ K^{1/(d-4)}$, where $K = m/H^{1-(2/d)}$. So we are left with the case where $K > 1$ and $\min(|x|,\ |y|) < c_1 K^{1/(d-4)}$.

Say $1 \leqq |y| \leqq c_1\ K^{1/(d-4)}$. It suffices to consider $1 \leqq |y| \leqq c_1\ m^{1/(d-4)} \leqq c_1 m^{2/d}$ if $d \geqq 8$. Given such a y, the number of solutions in x is (by Lemma 12C with $A = a,\ B = by^t,\ C = cy^d$)

$$\begin{aligned} &\ll 1 + \min\left(\left(\frac{m}{|A|}\right)^{1/d},\ \frac{m^{1/2}}{|C|^{(1/2)-(1/d)}}\right) \\ &\leqq 1 + \min\left(m^{1/d},\ \frac{m^{1/2}}{|y|^{(d/2)-1}}\right) . \end{aligned}$$

So for given y, the number of solutions is $\ll m^{1/d}$, and there are $\ll m^{2/d}$ solutions with $1 \leqq |y| \leqq m^{1/d}$. Now it remains to count those solutions with

$$m^{1/d} \leqq |y| \leqq c_1 m^{2/d} .$$

Their number is

$$\ll m^{2/d} + \sum_{m^{1/d} \leqq |y| \leqq c_1 m^{2/d}} \left(\frac{m^{1/2}}{|y|^{(d/2)-1}}\right) \tag{12.4}$$

We estimate the sum by considering the integral

$$\int_{m^{1/d}}^{c_1 m^{2/d}} \frac{1}{y^{(d/2)-1}} dy \ll m^{\frac{1}{d}(2-\frac{d}{2})} = m^{\frac{2}{d}-\frac{1}{2}} .$$

It is now easily seen that the sum in (12.4) is $\ll m^{2/d}$, and the proof is complete.

§13. Generalizations of the Thue Equation.

Let K be an algebraic number field of degree $[K : \mathbb{Q}] = \delta$. As usual, let $M(K)$ denote the set of absolute values on K and let S be a finite subset of $M(K)$, containing all of the Archimedean absolute values. Let $s =$ card (S) and for $\alpha \in K$, let $|\alpha|_S = \prod_{v \in S} |\alpha|_v^{n_v}$.

An element $\alpha \in K$ having $|\alpha|_v \leqq 1$ for every $v \notin S$ is called an *S-integer*. These integers form a subring $\mathfrak{O}_S$ of K. The units of $\mathfrak{O}_S$ form a group U_S consisting of $\alpha \in K$ with $|\alpha|_v = 1$ for every $v \notin S$.

Consider the special case where $S = M_\infty(K)$, i.e. the set of Archimedean absolute values of K. If the number field K has r_1 real embeddings and r_2 complex embeddings, then $s = r_1 + r_2$. In this case $\mathfrak{O}_S = \mathfrak{O}$, the ring of integers in K, and $U_S = U$, the group of units in K. By a generalized version of Dirichlet's Theorem, we know that U_S has rank $s - 1$, not just in the special case, but also for general S as above. The torsion part of U_S is finite and consists of the roots of unity in K. (The reader may find a proof of this version of Dirichlet's Unit Theorem in Borevich and Shafarevich (1966)).

Let $F(X, Y) \in \mathfrak{O}_S[X, Y]$ be a homogenous form of degree $d \geqq 3$. Suppose that F has no multiple factors. Consider the generalized Thue equation

$$|F(x, y)|_S = 1$$

in variables $x, y \in \mathfrak{O}_S$. Two pairs (x, y) and (x', y') are called equivalent if $x = x'\eta$, $y = y'\eta$ with $\eta \in U_S$. If (x, y) is a solution to the equation, then every pair which is equivalent to (x, y) is also a solution, since $|\eta|_S = 1$.

THEOREM 13A. *With conventions as above, the number of equivalence classes of solutions to*

$$|F(x, y)|_S = 1$$

is

$$\leqq (4s)^{2\delta}\ (4d)^{26s}\ .$$

This result, which will not be proved here, is due to Bombieri (1985).

COROLLARY 13B. *The number of equivalence classes of solutions to*

$$F(x, y) \in U_S$$

is

$$\leqq (4s)^{2\delta}\ (4d)^{26s}\ .$$

Now consider solutions to $F(x, y) = 1$ with $x, y \in \mathfrak{O}_S$. If (x, y) and (x', y') are solutions in the same equivalence class, then they differ by a factor $\eta \in U_S$. Since (by $F(x, y) = F(x', y') = 1$), $\eta^d = 1$, we have the following corollary.

COROLLARY 13C. *The number of solutions of*

$$F(x, y) = 1$$

with $x, y \in \mathfrak{O}_S$ is

$$\leqq d(4s)^{2\delta}\ (4d)^{26s}\ .$$

Now consider the equation

$$F(x, y) = p_1^{z_1} \cdots p_\nu^{z_\nu}$$

where $F(X, Y) \in \mathbb{Z}[X, Y]$ and $p_1, \ldots, p_\nu$ are distinct primes. We seek solutions x, y, $z_1, \ldots, z_\nu \in \mathbb{Z}$ with

$$gcd\ (x, y, p_i) = 1 \qquad (i = 1, \ldots, \nu).$$

This is known as the Thue-Mahler equation, since it is a generalization of the Thue equation which was first studied by Mahler (1933).

Example. We may seek integer solutions (x,y,z) of $x^3-2y^3=5^z$ where $gcd(x,y,5)=1$.

For the Thue-Mahler equation above, take $S=\{\infty,p_1,\dots,p_\nu\}$ with $s=\nu+1$. As in Corollary 13B, look for solutions to $F(x,y)\in U_S$ with $x,y\in\mathfrak{O}_S$. The corollary gives a bound on the number of equivalence classes of solutions. Two equivalent solutions differ by a factor in U_S, which consists of $\pm p_1^{w_1}\dots p_\nu^{w_\nu}$. Because of the condition $gcd(x,y,p_i)=1$, these factors can only be ± 1, and we have the following result.

COROLLARY 13D. *The number of solutions of the Thue-Mahler equation*

$$F(x,y)=p_1^{z_1}\dots p_\nu^{z_\nu}$$

is

$$\leqq 2\,(4\nu+4)^{2\delta}\,(4d)^{26(\nu+1)}\ .$$

This corollary includes the case $F(x,y)=m$, where $m=p_1^{z_1}\dots p_\nu^{z_\nu}$ is *given.* In this particular case, we know that, e.g., the factor 26 in the exponent is unnecessary. For lower bounds see Erdös, Stewart and Tijdeman (1988).

Next, we consider the Thue-Mahler Equation in terms of ideals in $\mathfrak{O}_S$. We know that the non-Archimdean absolute values in S come from prime ideals, say $\mathfrak{P}_1,\dots,\mathfrak{P}_t$. Then the group of units U_S consists of $\alpha\in K^*$ which generate a principal ideal $\langle\alpha\rangle$ of the form $\langle\alpha\rangle=\mathfrak{P}_1^{c_1}\dots\mathfrak{P}_t^{c_t}$. Above, we considered the equation $F(x,y)\in U_S$, but this can also be written as the generalized Thue-Mahler equation

$$\langle F(x,y)\rangle=\mathfrak{P}_1^{z_1}\dots\mathfrak{P}_t^{z_t}$$

in unknowns x,y in $\mathfrak{O}_S$ and $z_1,\dots,z_t$ in $\mathbb{Z}$.

Now consider the special case

$$\langle x^d-wy^d\rangle=\mathfrak{P}_1^{z_1}\dots\mathfrak{P}_t^{z_t}\ ,$$

where w is a given coefficient. Evertse (1984a) studied a variation of this, namely

$$\frac{\langle x^d-wy^d\rangle}{\langle x^d,\ wy^d\rangle}=\mathfrak{P}_1^{z_1}\dots\mathfrak{P}_t^{z_t}\ , \tag{13.1}$$

where $\langle\alpha,\beta\rangle$ is the fractional ideal generated by α and β. In this setting, one studies solutions $(x,y)\in\mathbb{P}^1(K)$ and $z_1,\dots,z_t\in\mathbb{Z}$. Evertse obtained the following result.

THEOREM 13E. *The number of solutions of (13.1) is no greater than* $(c_1d)^s$ *, where* c_1 *is an absolute constant.*

(Here $s=\operatorname{card}S$ *equals* t *plus the number of Archimedean absolute values).*

IV. S-unit Equations and Hyperelliptic Equations.

References: Evertse, Győry, Stewart and Tijdeman (1988), Shorey and Tijdeman (1986), Schlickewei (1977).

§1. S-unit Equations.

As in the end of Chapter III, let K be a number field with $[K : \mathbb{Q}] = \delta$. Also, $M_\infty(K) \subset S \subset M(K)$ and card $S = s$. An S-unit equation is one of the form $\alpha_1 x + \alpha_2 y = 1$, where non-zero $\alpha_1, \alpha_2 \in K$ are given, with unknowns $x, y \in U_S$.

Consider the concrete example where $K = \mathbb{Q}$ and $S = \{\infty, p_1, \dots, p_\nu\}$, with the equation

$$x + y = 1.$$

So we are looking at

$$\pm p_1^{z_1} \dots p_\nu^{z_\nu} \pm p_1^{w_1} \dots p_\nu^{w_\nu} = 1 \ ,$$

where $z_i, w_i \in \mathbb{Z}$, $(i = 1, \dots, \nu)$. Write $x = x'/z'$ and $y = y'/z'$ with $gcd\,(x', y', z') = 1$. Then we have

$$x' + y' = z' \ ,$$

or

$$\pm p_1^{z_1} \dots p_\nu^{z_\nu} \pm p_1^{w_1} \dots p_\nu^{w_\nu} \pm p_1^{t_1} \dots p_\nu^{t_\nu} = 0 \ ,$$

where z_i, w_i, t_i $(i = 1, \dots, \nu)$ are nonnegative integers and the summands have no common prime factor. (Thus min $(z_i, w_i, t_i) = 0$ $(i = 1, \dots, \nu)$).

$$\text{Example: } \pm 2^{z_1} 3^{z_2} \pm 2^{w_1} 3^{w_2} \pm 2^{t_1} 3^{t_2} = 0 \ .$$

THEOREM 1A. *An S-unit equation $\alpha_1 x + \alpha_2 y = 1$ has at most a finite number of solutions. Furthermore, if $\alpha_1, \alpha_2 \in U_S$, then their number is*

$$\leqq s^{2\delta} c^S \ ,$$

where c is an absolute constant.

Remark. We may force $\alpha_1, \alpha_2 \in U_S$ by enlarging S if necessary. This may change the bound, though. In section 2, we will give bounds which do not require $\alpha_1, \alpha_2 \in U_S$.

We follow Evertse, Győry, Stewart and Tijdeman (1988).

Proof. We prove the second assertion, since it implies the first. By a generalized version of Dirichlet's Unit Theorem mentioned in Chapter III, the group of units U_S has the form

$$U_S = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{\leftarrow\ s-1 \text{ times} \rightarrow} \oplus \, (\text{Torsion}) \ ,$$

where the torsion part is a finite cyclic group consisting of roots of unity.

Let U_S^d be the subgroup of U_S consisting of elements of the form u^d where $u \in U_S$. The quotient group U_S/U_S^d has cardinality $\leqq d^{s-1}$. $d = d^s$. Let $\zeta_1, \dots, \zeta_\ell$ be coset representatives, where $\ell \leqq d^s$. Then any $x, y \in U_S$ may be written as

$$x = \zeta_i X^d \qquad \text{and} \qquad y = \zeta_j Y^d ,$$

where $X, Y \in U_S$ and $1 \leqq i,\ j \leqq \ell$. The S-unit equation $\alpha_1 x + \alpha_2 y = 1$ becomes

$$\alpha_1 \zeta_i X^d + \alpha_2 \zeta_j\ Y^d = 1 .$$

Applying the argument for Corollary 13C of Chapter III with any given $d \geqq 3$, but noting that factors η with η^d do not affect $x = \xi_i (X\eta)^d$ and $y = \xi_j (Y_\eta)^d$, we see that the total number of solutions is

$$\leqq \ell^2\ (4s)^{2\delta}\ (4d)^{26s} \leqq d^{2s} (4s)^{2\delta}\ (4d)^{26s}.$$

For instance, if $d = 3$, we get the bound

$$3^{2s}\ (12)^{26s}\ (4s)^{2\delta} \leqq s^{2\delta} (12)^{28s}\ 4^{2\delta} < s^{2\delta}\ 12^{30s} .$$

So we have used the fact that a Thue equation has only finitely many solutions, to show that an S-unit equation has only finitely many solutions as well. One can see that the converse is also true, i.e. that the finiteness of the number of solutions of S-unit equations implies the finiteness for Thue equations. We consider the Thue equation

$$F(x, y) = m ,$$

where $F(X, Y) \in \mathfrak{O}_S[X, Y]$ is homogeneous with at least three non-proportional linear factors and $m \in \mathfrak{O}_S$.

In some extension, F factors as

$$F = L_1 \dots L_d ,$$

where the L_i are linear with coefficients in a field $N \supset K \supset \mathbb{Q}$. Let $S' \subset M(N)$ consist of the extensions of the absolute values of S to N. We can assume that m and the coefficients of L_i lie in $\mathfrak{O}_{S'}$. Consider the equation

$$L_1(\underline{x}) \dots L_d(\underline{x}) = m \tag{1.1}$$

and seek solutions $x, y \in \mathfrak{O}_{S'}$.

Take linear forms L_1, L_2, L_3 which are non-proportional. Since these are three linear forms in two variables, they must be linearly dependent. We have

$$L_3 = \lambda_1\ L_1 + \lambda_2 L_2 \qquad \text{with} \qquad \lambda_1, \lambda_2 \in N^\times ,$$

and

$$\lambda_1\ \frac{L_1(\underline{x})}{L_3(\underline{x})} + \lambda_2 \frac{L_2\ (\underline{x})}{L_3(\underline{x})} = 1 .$$

By (1.1) above, we know that $L_1(\underline{\underline{x}}) \mid m$ in $\mathfrak{O}_{S'}$. Up to equivalence, there are only finitely many divisors of m. Say $L_1(\underline{\underline{x}}) = \rho u$, where $u \in U_{S'}$, and there are only finitely many possibilities for ρ. Then

$$\frac{L_1(\underline{\underline{x}})}{L_3(\underline{\underline{x}})} = \rho_1 \; u_1$$

where $u_1 \in U_{S'}$ and there are only finitey many choices for ρ_1. Similarly,

$$\frac{L_2(\underline{\underline{x}})}{L_3(\underline{\underline{x}})} = \rho_2 \; u_2.$$

This gives

$$\lambda_1\rho_1 u_1 + \lambda_2\rho_2 u_2 = 1$$

with $u_1, u_2 \in U_{S'}$. This is an S'-unit equation in u_1, u_2, and it has only finitely many solutions. Thus there are only finitely many possibilities for $L_1(\underline{\underline{x}})/L_3(\underline{\underline{x}})$ and $L_2(\underline{\underline{x}})/L_3(\underline{\underline{x}})$. But these quotients determine $\underline{\underline{x}}$ up to a factor of proportionality. It now follows immediately that (1.1) has only finitely many solutions $\underline{\underline{x}}$.

§2. Evertse's Bound.

Let K be a number field with $[K : \mathbb{Q}] = \delta$ and $S \subset M(K)$ with card $S = s$, as before. Evertse (1983) gives a bound for the number of solutions of the S-unit equation

$$\alpha_1 x + \alpha_2 y = 1$$

which is independent of the coefficients α_1, α_2 and which does not require that $\alpha_1,\ \alpha_2 \in U_S$.

THEOREM 2A. *(Evertse (1984)) The equation*

$$\alpha_1 x + \alpha_2 y = 1,$$

where $\alpha_1, \alpha_2 \in K$ are non-zero has at most

$$3 \cdot 7^{\delta+2s}$$

solutions $x,\ y$ in U_S.

Here, we will prove less, namely that the number of solutions is

$$\leqq c_1(\delta) c_2^s.$$

For instance, if $K = \mathbb{Q}$, then the number is $\leqq c_3^s$.

First we reformulate the problem in projective space. That is, we look at solutions to the equation

$$\alpha_1 x + \alpha_2 y - z = 0,$$

where $(x, y, z) \in \mathbb{P}^2(U_S)$. Or let $\alpha_3 = -1$ and consider

$$\alpha_1 x + \alpha_2 y + \alpha_3\ z = 0,$$

which may be rewritten as

$$y_1 + y_2 + y_3 = 0\ .$$

Then we consider solutions where $y_i/\alpha_i \in U_S \quad (i = 1, 2, 3)$, and proportional solutions are considered the same.

Let $\underline{\underline{\alpha}} = (\alpha_1, \alpha_2, \alpha_3)$ and $\underline{\underline{y}} = (y_1, y_2, y_3)$. As in Chapter I, let $\langle \xi \rangle_v = |\xi|_v^{n_v}$, and define

$$A = \prod_{v \notin S} \frac{\langle \underline{\underline{\alpha}} \rangle_v^3}{\langle \alpha_1 \alpha_2 \alpha_3 \rangle_v}\ .$$

Since $|y_i/\alpha_i|_v = 1$ for $v \notin S$, we have

$$\prod_{v \in S} \frac{\langle y_1 y_2 y_3 \rangle_v}{\langle \underline{\underline{y}} \rangle_v^3} = \prod_{v \in S} \frac{1}{\langle \underline{\underline{y}} \rangle_v^3} \prod_{v \notin S} \frac{1}{\langle y_1 y_2 y_3 \rangle_v} \prod_{v \notin S} \left(\frac{\langle \underline{\underline{\alpha}} \rangle_v^3}{\langle \underline{\underline{y}} \rangle_v^3} \frac{\langle y_1 y_2 y_3 \rangle_v}{\langle \alpha_1 \alpha_2 \alpha_3 \rangle_v} \right)$$

$$= A\ H_k(\underline{\underline{y}})^{-3}\ .$$

Given $\underline{\underline{y}}$ and v, let (i_v, j_v, k_v) be the permutation of $(1, 2, 3)$ with the property that $|y_{i_v}|_v \leqq |y_{j_v}|_v \leqq |y_{k_v}|_v$. If v is non-Archimedean, then $|y_{j_v}|_v = |y_{k_v}|_v$ since $y_{i_v} + y_{j_v} + y_{k_v} = 0$. If v is Archimedean, then $|y_{k_v}|_v \leqq 2|y_{j_v}|_v$ and $|\underline{\underline{y}}|_v \leqq \sqrt{6}|y_{j_v}|_v$. This gives

$$\frac{|y_{i_v}|_v}{|\underline{\underline{y}}|_v} \leqq c_v \frac{|y_1 y_2 y_3|_v}{|\underline{\underline{y}}|_v^3}\ ,$$

where

$$c_v = \begin{cases} 1 & \text{if } v \text{ is non-Archimedean,} \\ \sqrt{6} & \text{if } v \text{ is Archimedean.} \end{cases}$$

Then we have

$$\prod_{v \in S} \frac{\langle y_{i_v} \rangle_v}{\langle \underline{\underline{y}} \rangle_v} < 3^\delta\ A\ H_k(\underline{\underline{y}})^{-3}\ . \tag{2.1}$$

This ties in with Roth's Theorem in its generalized form, that is, Theorem 10B of Chapter II. We consider the variables as y_1, y_2, and we have the linear forms

$$L_v = \begin{cases} y_1 & \text{if} \quad i_v = 1 \\ y_2 & \text{if} \quad i_v = 2 \\ -y_1 - y_2 & \text{if} \quad i_v = 3 \end{cases}\ .$$

We know that

$$\max\left(|y_1|_v,\ |y_2|_v,\ |y_1 + y_2|_v\right) \leqq 2^{\lambda(v)} \max\left(|y_1|_v,\ |y_2|_v\right),$$

where

$$\lambda(v) = \begin{cases} 0 & \text{if } v \text{ is non-Archimedean} \\ 1 & \text{if } v \text{ is Archimedean .} \end{cases}$$

Letting $\underline{\underline{x}} = (y_1,\ y_2)$, the inequality becomes

$$\langle \underline{\underline{x}} \rangle_v \geqq 2^{-\lambda(v)n_v} \langle \underline{\underline{y}} \rangle_v \ .$$

Then (2.1) yields

$$\prod_{v \in S} \frac{\langle L_v(\underline{\underline{x}})\rangle_v}{\langle L_v \rangle_v \langle \underline{\underline{x}} \rangle_v} < 6^\delta\ A\ H_K(\underline{\underline{x}})^{-3} \tag{2.2}$$

since $\langle L_v \rangle_v \geqq 1$.

To count solutions, we apply Theorem 10B of Chapter II. We get

$$\leqq c_3(\delta, t, \varepsilon)\ c_4(\varepsilon)^s$$

solutions with

$$H_K(\underline{\underline{x}}) > c_1(\delta, t, \varepsilon)\ (C + H + 1)^{c_2(\delta,t,\varepsilon)}\ ,$$

where t is the number of distinct linear forms L_v, so that $t = 3$, and $\varepsilon = 1,\ C = 12^\delta A$. So we have

$$\leqq c_3(\delta) c_4^\delta$$

solutions with

$$H_K(\underline{\underline{x}}) > c_1(\delta)\ (12^\delta A + 2 + 1)^{c_2(\delta)}\ .$$

Now we are left to count small solutions. We have

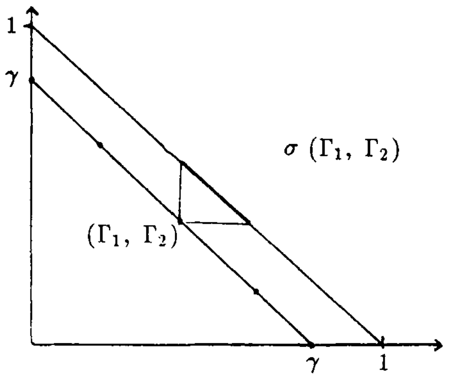
$$H_K(\underline{\underline{x}}) \leqq H_K(\underline{\underline{y}}) \leqq 2^\delta H_K(\underline{\underline{x}})\ ,$$

and there are two possibilities. If $A \leqq 12^{12\delta}$, then $H_K(\underline{\underline{y}}) \leqq c_5(\delta)$. There are only finitely many solutions in this case, say $\leqq c_6(\delta)$. Then we are left with the case where $A > 12^{12\delta}$, and we have to count solutions with $H_K(\underline{\underline{y}}) < A^{c_7(\delta)}$. To do this, we need the following lemma.

LEMMA 2B. *Suppose $0 < \gamma < 1$ and $s \in \mathbb{Z}^+$ are given. Then there is a finite set $\mathfrak{S}$ of s-tuples $(\Gamma_1, \dots, \Gamma_s)$ of non-negative reals with $\Gamma_1 + \dots + \Gamma_s = \gamma$, such that for every $\underline{\underline{x}} = (x_1, \dots, x_s)$ with $x_i \geqq 0$, there is an s-tuple from $\mathfrak{S}$ with $x_i \geqq \Gamma_i(x_1 + \dots + x_s) \quad (i = 1, \dots, s)$. Furthermore, $\operatorname{card} \mathfrak{S} \leqq c_8(\gamma)^s$.*

Exercise 2a. Prove Lemma 2B.

In the case $s = 2$, the elements of $\mathfrak{S}$ lie on the line $\Gamma_1 + \Gamma_2 = \gamma$. We have the following picture.



It is easy to see that one may cover the line $x_1 + x_2 = 1$ with a finite number of sets $\sigma = \sigma(\Gamma_1, \Gamma_2)$ consisting of (x_1, x_2) with $x_i \geqq \Gamma_i \quad (i = 1, 2)$. The lemma then follows for the case $s = 2$.

Remark. As a consequence of this lemma, we have that for $x_i \leqq 0, \quad (i = 1, \dots, n)$, there is some $(\Gamma_1, \dots, \Gamma_s) \in \mathfrak{S}$ such that $x_i \leqq \Gamma_i(x_1 + \dots + x_s) \quad (i = 1, \dots, s)$.

To finish counting solutions, we will apply the lemma with $\gamma = 5/6$ and $s = \text{card } S$. Then for every $\underline{\underline{y}} = (y_1, y_2, y_3)$, there will be some $(\Gamma_1, \dots, \Gamma_s) \in \mathfrak{S}$ with

$$\frac{\langle y_{i_v} \rangle_v}{\langle \underline{\underline{y}} \rangle_v} \leqq \left(\prod_{v \in S} \frac{\langle y_{i_v} \rangle_v}{\langle \underline{\underline{y}} \rangle_v} \right)^{\Gamma_v} \tag{2.3}$$

for every $v \in S$. (Notice that we have changed the subscripts of $\Gamma_i \; (i = 1, \dots, s)$ to $\Gamma_v \; (v \in S)$.) Using the estimates (2.2), (2.3), we have

$$\frac{\langle y_{i_v} \rangle_v}{\langle \underline{\underline{y}} \rangle_v} \leqq \left(6^\delta A \; H_K(\underline{\underline{y}})^{-3} \right)^{\Gamma_v} \qquad (v \in S). \tag{2.4}$$

We subdivide the set of solutions into those with fixed $\{\Gamma_v\}_{v \in S}$, which gives $\leqq c_8(\gamma)^s = c_9^s$ classes. We then further subdivide into classes for which i_v is fixed for every $v \in S$, which gives 3^s subclasses. All together, we have c_{10}^S classes. In the next lemma, we establish a Gap Principle which allows us to count the number of solutions in a fixed class.

LEMMA 2C. *Consider solutions $\underline{\underline{y}}$, $\underline{\underline{y}}'$ to (2.4) which lie in a given class. Suppose $H_K(\underline{\underline{y}}) \leqq H_K(\underline{\underline{y}}')$. Then*

$$H_K(\underline{\underline{y}}') \geqq 12^{-\delta} \, A^{1/6} \; H_K(\underline{\underline{y}})^{3/2} \, .$$

Proof. Write $\underline{\underline{y}} = (y_1, y_2, y_3)$ and $y' = (y'_1, y'_2, y'_3)$. For $v \in M(K)$, form the "determinant"

$$\Delta_v = \frac{\langle y_i y'_j - y_j y'_i \rangle_v}{\langle \underline{\underline{y}} \rangle_v \ \langle \underline{\underline{y}}' \rangle_v}$$

where $i \neq j$. (Since $\sum y_i = \sum y'_i = 1$, it doesn't matter which pair $i \neq j$ we choose).

In particular, for $v \in S$, take $i = i_v$. Then

$$\Delta_v \leqq 2^{\lambda(v) n_v} \ \max \left(\frac{\langle y_{i_v} \rangle_v}{\langle \underline{\underline{y}} \rangle_v}, \ \frac{\langle y'_{i_v} \rangle_v}{\langle \underline{\underline{y}}' \rangle_v} \right),$$

where

$$\lambda(v) = \begin{cases} 1 & \text{if } v \text{ is Archimedean} \\ 0 & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

Then, by (2.4), we have

$$\Delta_v \leqq 2^{\lambda(v) n_v} \left(6^\delta A \ H_K(\underline{\underline{y}})^{-3} \right)^{\Gamma_v} ,$$

where $\sum_{v \in S} \Gamma_v = 5/6$. Taking the product over $v \in S$, we get

$$\prod_{v \in S} \Delta_v \leqq 2^\delta \left(6^\delta A \ H_K(\underline{\underline{y}})^{-3} \right)^{5/6} . \tag{2.5}$$

Now, for $v \neq S$, we have $|y_i/\alpha_i|_v = 1$ since $y_i/\alpha_i \in U_S$. A similar result holds for $\underline{\underline{y}}'$, so then

$$\langle y_i \rangle_v = \langle y'_i \rangle_v = \langle \alpha_i \rangle_v, \qquad (i = 1, 2, 3).$$

If we pick i, j, k such that

$$\langle \alpha_i \rangle_v \leqq \langle \alpha_j \rangle_v \leqq \langle \alpha_k \rangle_v = \langle \underline{\underline{\alpha}} \rangle_v \ ,$$

then

$$\Delta_v \leqq \frac{\langle \alpha_i \rangle_v \ \langle \alpha_j \rangle_v}{\langle \underline{\underline{\alpha}} \rangle_v^2} = \frac{\langle \alpha_i \alpha_j \alpha_k \rangle}{\langle \underline{\underline{\alpha}} \rangle_v^3}$$

where the inequality holds since $v \notin S$ is a non-Archimedean absolute value. Taking the product over $v \notin S$ gives

$$\prod_{v \notin S} \Delta_v \leqq \prod_{v \notin S} \frac{\langle \alpha_i \alpha_j \alpha_k \rangle_v}{\langle \underline{\underline{\alpha}} \rangle_v^3} = A^{-1} .$$

In conjunction with (2.5) this yields

$$\frac{1}{H_K(\underline{\underline{y}}) \ H_K(\underline{\underline{y}}')} = \prod_{v \in M(K)} \Delta_v \leqq 12^\delta \ A^{-1/6} \ H_K(\underline{\underline{y}})^{-5/2} .$$

Lemma 2C follows.

We return to the proof of Theorem 2A, where we were left with solutions having $H_K(\underline{\underline{y}}) \leqq A^{c_7(\delta)}$. Furthermore, we may initially restrict ourselves to solutions in a given class, as explained above. For two such solutions $\underline{\underline{y}}$, $\underline{\underline{y}}'$, the Gap Principle of Lemma 2C, along with $A \geqq 12^{12\delta}$, gives the inequality $H_K(\underline{\underline{y}}') \geqq A^{1/12}\ H_K(\underline{\underline{y}})^{3/2}$. Suppose some fixed class contains solutions $\underline{\underline{y}}_0$, $\underline{\underline{y}}_1, \ldots, \underline{\underline{y}}_\nu$ with non-decreasing heights bounded above by $A^{c_7(\delta)}$. Then by the Gap Principle,

$$H_K(\underline{\underline{y}}_1) \geqq A^{1/12}, \ldots , H_K(\underline{\underline{y}}_\nu) \geqq (A^{1/12})^{(3/2)^{\nu-1}} .$$

But $H_K(\underline{\underline{y}}_\nu) \leqq A^{c_7(\delta)}$, so we have

$$\frac{1}{12}\left(\frac{3}{2}\right)^{\nu-1} \leqq c_7(\delta) ,$$

and $\nu \leqq c_{11}(\delta)$.

Recall that the number of classes was not greater than c_{10}^s, so that we have no more than $c_{11}(\delta)c_{10}^s$ solutions with height bounded by $A^{c_7(\delta)}$. Combining this with the other estimates, we get no more than $c_1(\delta)c_2^s$ solutions to the S-unit equation, where $\delta = [K : \mathbb{Q}]$ and $s =$ card S. Our proof essentially followed the method of Evertse, Győry, Stewart and Tijdeman (1988).

Evertse's proof of Theorem 2A used hypergeometric functions. These are advantageous when studying rational approximations to radicals, i.e. numbers of the type $\sqrt[d]{r}$.

§3. More on S-unit Equations.

In sections 1 and 2, we considered S-unit equations in two variables. We reformulate this in projective space by considering the equation

$$\alpha_1\ x_1 + \alpha_2\ x_2 + \alpha_3\ x_3 = 0 ,$$

where $\alpha_1, \alpha_2, \alpha_3 \in K^*$ are given and the solutions (x_1, x_2, x_3) lie in $\mathbb{P}^2(U_S)$. Even more generally, we may consider

$$\alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_n x_n = 0 ,$$

where $\alpha_i \in K^* \quad (i = 0, \ldots , n)$ and where we seek solutions $(x_0, \ldots , x_n) \in \mathbb{P}^n(U_S)$.

If $n \geqq 3$, we no longer necessarily have only finitely many solutions. Consider, for instance, the following example. Let $n = 3$ and consider solutions of the equation $x_1 + x_2 + x_3 + x_4 = 0$, where $S = \{\infty, 2\}$ and the number field $K = \mathbb{Q}$. There are infinitely many solutions of the form $(2^n, -2^n, 2^m, -2^m)$ where $m, n \in \mathbb{Z}$.

However, with suitable restrictions on the solutions, an S-unit equation will have only finitely many solutions. We see this in the following theorem due to Evertse (1984b) and Schlickewei and van der Poorten (1982).

THEOREM 3A. *An S-unit equation has only finitely many solutions in $\mathbb{P}^n(U_S)$ for which no subsum vanishes, i.e. for which $\alpha_{i_1}x_{i_1}+\ldots+\alpha_{i_t}x_{i_t} \neq 0$ for any $\{i_1, i_2, \ldots, i_t\} \subset \{0, 1, \ldots, n\}$ with $t \neq 0$, $t \neq n+1$.*

The proof, which will not be given here, (but see Ch. V, §2), uses results on simultaneous diophantine approximations which involve both Archimedean and non-Archimedean absolute values. Mahler (1933) was the first to study diophantine approximations using non-Archimedean absolute values.

For the remainder of this section we return to the case $n = 2$, considering equations of the type

$$\alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2 = 0 \qquad (3.1).$$

Evertse, Györy, Stewart, and Tijdeman defined an equivalence relation on S-unit equations. A slight variation on their definition is that two equations (3.1) and

$$\alpha'_0 x_0 + \alpha'_1 x_1 + \alpha'_2 x_2 = 0 \qquad (3.2).$$

are *equivalent* if

$$\alpha'_i = \lambda \varepsilon_i \alpha_i \qquad (i = 0, 1, 2),$$

where $\varepsilon_i \in U_S$ and $\lambda \in K^\times$. Equivalent equations have the same number of S-unit solutions, for if x_0, x_1, x_2 is a solutions of (3.1), then $x_0/\varepsilon_0, x_1/\varepsilon_1, x_2/\varepsilon_2$ is a solution of (3.2).

THEOREM 3B. (Evertse, Györy, Stewart, Tijdeman (1988)). *Except for finitely many equivalence classes of equations, an S-unit equation over $\mathbb{P}^2(U_S)$ has at most two solutions.*

Remark. In general, there may be more solutions. Consider the S-unit equation $x + y = 1$. Nagell (1969) proved that when $\delta \geqq 5$, there are number fields K of degree δ such that this equation has at least $3(2\delta - 3)$ solutions in units of K, i.e. with $S = M_\infty(K)$. In a more recent result, Erdös, Stewart and Tijdeman (1988) proved that for $K = \mathbb{Q}$ and s arbitrary, there are sets S of cardinality s such that the S-unit equation above has at least $e^{cs^{1/2}/\log s}$ solutions. Stewart made a case that $e^{s^{2/3}}$ is the correct order.

Remark. The number 2 in Theorem 3B is best possible, provided $s > 1$, so that U_S is infinite. To see this, pick $\xi, \eta \in U_S$, with $\xi \neq \eta$, $\xi \neq 1$, $\eta \neq 1$. Consider the equation

$$\alpha_1 x + \alpha_2 y = 1,$$

where $\alpha_1 = (\eta - 1)/(\eta - \xi)$ and $\alpha_2 = (\xi - 1)/(\xi - \eta)$. This has solutions (1, 1) and (ξ, η). Since there are infinitely many choices for ξ, η, there are infinitely many S-unit equations of this particular form. However, only a finite number of these belong to a given class. To see this, suppose

$$\alpha_1 x + \alpha_2 y = 1$$

and

$$\alpha'_1 x + \alpha'_2 y = 1$$

lie in the same class. Then $\alpha_1' = \alpha_1\varepsilon_1$ and $\alpha_2' = \alpha_2\varepsilon_2$ where $\varepsilon_1, \varepsilon_2 \in U_S$. Then the second equation becomes $\alpha_1\varepsilon_1 x + \alpha_2\varepsilon_2 y = 1$. Since (1,1) is a solution of this new equation, we have

$$\alpha_1\varepsilon_1 + \alpha_2\varepsilon_2 = 1 \ .$$

But this is an S-unit equation in the unknowns $\varepsilon_1, \varepsilon_2$, thus it has only finitely many solutions. Therefore, we have infinitely many equivalence classes of equations with at least two solutions.

Proof of Theorem 3B. We are considering S-unit equations of the form

$$\alpha x + \beta y + \gamma z = 0 \ ,$$

with solutions $(x, y, z) \in \mathbb{P}^2(U_S)$. Every equivalence class of equations contains an equation of the type

$$\alpha x + \beta y + z = 0 \ .$$

Now suppose that we have three distinct solutions, say (x_i, y_i, z_i) $(i = 1, 2, 3)$. Thus

$$\alpha x_i + \beta y_i + z_i = 0 \qquad (i = 1, 2, 3). \tag{3.3}$$

Because the solutions are distinct in $\mathbb{P}^2(K)$, any two of the triples (x_i, y_i, z_i) are non-proportional. So we have

$$\operatorname{rank}\begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix} = 2,$$

and then

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} \neq 0, \tag{3.4}$$

by (3.3). Therefore, $x_1y_2z_3 \neq x_2y_1z_3$. Cyclic permutations give two more relations, namely $x_2y_3z_1 \neq x_3y_2z_1$ and $x_3y_1z_2 \neq x_1y_3z_2$. All together, considering y, z or z, x in place of x, y in (3.4), we get nine relations. Also, the three solutions to the given S-unit equation satisfy (3.3), which may be interpreted as a system of three equations for α, β, γ. The matrix of this system must be singular:

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0 \ .$$

Writing out this determinant, we have

$$x_1y_2z_3 + x_2y_3z_1 + x_3y_1z_2 - x_1y_3z_2 - x_2y_1z_3 - x_3y_2z_1 = 0, \tag{3.5}$$

and the nine relations above impose the additional condition that no term with a + sign can equal a term with a − sign.

To finish the proof, we need the following lemma.

LEMMA 3C. *There are only finitely many possibilities for the ratios* x_1z_2/x_2z_1 *and* y_1z_2/y_2z_1.

Proof. The relation (3.5) is about a sum of S-units, i.e. an equation

$$a_1 + a_2 + a_3 - b_1 - b_2 - b_3 = 0,$$

with $a_i, b_i \in U_S \quad (i = 1,2,3)$. By Theorem 3A, this equation has only a finite number of solutions in $\mathbb{P}^5(U_S)$ for which no subsum vanishes. We consider several cases.

case (i). Suppose no subsum vanishes. Then we have only finitely many possibilities for

$$b_1/a_2 = x_1y_3z_2/x_2y_3z_1 = x_1z_2/x_2z_1$$

and

$$a_3/b_3 = x_3y_1z_2/x_3y_2z_1 = y_1z_2/y_2z_1.$$

case (ii). Suppose $a_1 + a_2 + a_3 = 0$ and $b_1 + b_2 + b_3 = 0$. For each of these subsums, we may apply Theorem 3A to see that there are only finitely many possibilities for a_1/a_2, a_3/a_2, b_1/b_2, b_1/b_3. Then there are only finitely many possibilities for the product $a_1a_3b_1^2/a_2^2b_2b_3$, which simplifies to $(x_1z_2/x_2z_1)^3$. So we have only finitely many possibilities for x_1z_2/x_2z_1, as desired. By symmetry, we get the same result for y_1z_2/y_2z_1.

Again by symmetry, we are left with the following two cases.

case (iii). $a_1 + a_2 = 0$ and $a_3 - b_1 - b_2 - b_3 = 0$.

case (iv). $a_1 + a_2 - b_1 = 0$ and $a_3 - b_2 - b_3 = 0$.

Exercise 3a. Establish the result for cases (iii) and (iv).

We return to the proof of Theorem 3B. From (3.3) with $i = 1,2$ we obtain

$$\alpha = \frac{-\begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}}{\begin{vmatrix} y_1 & x_1 \\ y_2 & x_2 \end{vmatrix}}, \qquad \beta = \frac{\begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix}}{\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}},$$

so that

$$\alpha\frac{x_1}{z_1} = -\frac{(y_1z_2/y_2z_1) - 1}{(x_2y_1/x_1y_2) - 1}, \ \beta\frac{y_1}{z_1} = \frac{(x_1z_2/x_2z_1) - 1}{(x_1y_2/x_2y_1) - 1}.$$

Thus, by Lemma 3C, there are only finitely many choices for $\alpha x_1/z_1$ and $\beta y_1/z_1$. Since x_1/z_1, $y_1/z_1 \in U_S$, there are only finitely many possibilities for α, β up to equivalence classes (i.e. up to S-units). Therefore, there are, up to equivalence, only finitely many S-unit equations with more than two solutions.

Remark. This argument can not be generalized to give a similar result for S-unit equations in four variables.

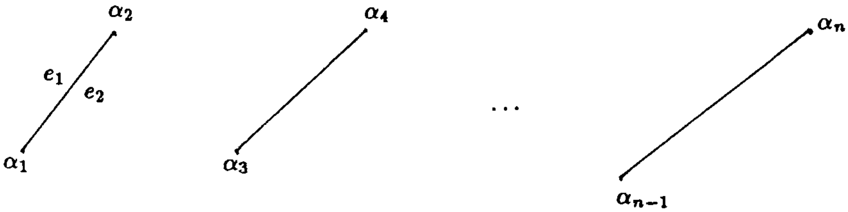
Remark. The number of exceptional equivalence classes has not been estimated, although such an estimate could perhaps be derived from recent bounds on the number of solutions of S-unit equations in n variables.

§4. Elliptic, Hyperelliptic, and Superelliptic Equations.

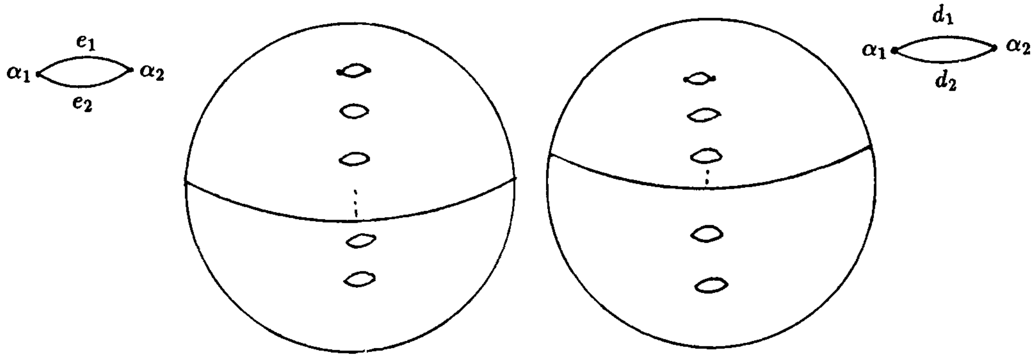
We consider equations of the form $y^d = f(x)$, where $d \geqq 2$, $\deg f = n \geqq 2$ and $\Delta(f) = \operatorname{discr}(f) \neq 0$. The case where $d = n = 2$ will be excluded. The polynomial f may have its coefficients in various fields or rings, for example, $f(X) \in \mathbb{Q}[X]$, or $f(X) \in K[X]$ where K is a number field, or $f(X) \in \mathfrak{O}_S[X]$ where $\mathfrak{O}_S$ is as before.

In the case $d = 2$, $n = 3$, we have *elliptic equations*, which have the form $y^2 = f(x)$, where f is a cubic polynomial with distinct roots. When $d = 2$ and $\deg f = n \geqq 3$, we have ***hyperelliptic equations***. The most general case, namely $y^d = f(x)$, where $d \geqq 2$, $n \geqq 2$, but n and d not both 2 is called a ***superelliptic equation***.

In the case of hyperelliptic equations, the genus of the Riemann surface is $g = [(n-1)/2]$. For suppose the equation is written in factored form as $y^2 = a(x-\alpha_1)\dots(x-\alpha_n)$. Consider the case where n is even, say $n = 2m$. Since n is even, we may pair the roots, as shown, making a cut between each pair.



We see that y is an analytic function in this cut plane. In other words, we have two Riemann spheres with m cuts in each.



Identifying edges of the various cuts, we get a single Riemann surface which is homomorphic to the surface of a pretzel with $m-1$ "holes". We have to identify, e.g., the upper edge e_1 with the lower edge d_2, and the lower edge e_2 with the upper edge d_1. Thus the genus is $m - 1 = [(2m-1)/2] = [(n-1)/2]$. The proof is the same for n odd, except that the last root is paired with the point at infinity on the sphere.

Exercise 4a. Consider the equation $y^3 = f(x)$, where f is a cubic polynomial with distinct roots. Show the genus $g = 1$.

THEOREM 4A. *A superelliptic equation with coefficients in an algebraic number field K has only finitely many solutions $x, y \in \mathfrak{O}_S$. (Here $S \subset M(K)$ and $\mathfrak{O}_S$ are as before.)*

The special case of an elliptic equation was done by Mordell (1922). The general case, which is due to Siegel (1926), was published under the pseudonym X.

In the proof it is necessary to consider an extension field $K' \supset K$. We then choose $S' \subset M(K')$ large, in particular so large that it contains every extension of elements of S to the field K'. Then if $x \in K$ is an S-unit, it is also an S'-unit. For if $|x|_v = 1$ for every $v \notin S$, then $|x|_w = 1$ for every $w \notin S'$.

Proof. In some extension field K', the polynomial f factors, i.e.

$$y^d = a(x - \alpha_1)\dots(x - \alpha_n), \tag{4.1}$$

with $a, \alpha_i \in K'$, provided K' is sufficiently large. Furthermore, if S' is large enough, then $a, \alpha_i \in \mathfrak{O}_{S'}$. By a change of notation, we may suppose that K, S have these properties. We will use the following lemma to rewrite the factors $x - \alpha_i$.

LEMMA 4B. *There exists a finite set B of non-zero elements of K such that for any solution x, y to (4.1) with $y \neq 0$, we have*

$$x - \alpha_i = \beta_i y_i^d,$$

where $\beta_i \in B$ and $y_i \in \mathfrak{O}_S$.

Proof.

(i) There is a finite subset $\xi_1, \dots, \xi_m$ in U_S such that every $u \in U_S$ may be written in the form
$$u = \xi_i u'^d,$$
where $1 \leqq i \leqq m$ and $u' \in U_S$.

(ii) Let P be the set of prime ideals in $\mathfrak{O}_S$ which either divide $\alpha_i - \alpha_j$ for some $i \neq j$ or divide a. Then P is finite. Suppose some prime ideal $\mathfrak{P}$ divides $x - \alpha_i$ and $x - \alpha_j$ for $i \neq j$. Then $\mathfrak{P} \in P$.

(iii) Say P consists of $\mathfrak{P}_1, \dots, \mathfrak{P}_\ell$. If $\mathfrak{B}$ is an ideal whose prime factors lie in P, then $\mathfrak{B} = \mathfrak{P}_1^{c_1} \dots \mathfrak{P}_\ell^{c_\ell} (\mathfrak{P}_1^{t_1} \dots \mathfrak{P}_\ell^{t_\ell})^d$, where $0 \leqq c_i < d$ for $i = 1, \dots, \ell$. In other words, $\mathfrak{B} = \mathfrak{B}^* \mathfrak{Q}^d$ with only finitely many possibilities for $\mathfrak{B}^*$.

(iv) We know that the class number h of the ring $\mathfrak{O}_S$ is finite. This means that there are certain fractional ideals $\mathfrak{D}_1, \dots, \mathfrak{D}_h$ such that every ideal has the form
$$\mathfrak{D}_i \langle z \rangle,$$
where $\langle z \rangle$ denotes the principal fractional ideal generated by $z \in K$ and where $1 \leqq i \leqq h$. If the $\mathfrak{D}_i$ are properly chosen, then any integral ideal $\mathfrak{D}$ will have the form
$$\mathfrak{D} = \mathfrak{D}_i \langle z \rangle,$$
where now $z \in \mathfrak{O}_S$.

We now combine these observations. For $x-\alpha_i$ given, write $\langle x-\alpha_i\rangle = \mathfrak{A}_i\mathfrak{B}_i$, where $\mathfrak{A}_i$ consists of prime factors which are not in P and B_i consists of prime factors which are in P. Then we have

$$\begin{aligned}\langle y\rangle^d &= \langle a\rangle\ \langle x-\alpha_1\rangle\ldots\langle x-\alpha_n\rangle\\ &= \langle a\rangle\mathfrak{A}_1\ldots\mathfrak{A}_n\mathfrak{B}_1\ldots\mathfrak{B}_n,\end{aligned}$$

where each $\mathfrak{A}_i$ is coprime to the other factors on the right-hand side by remark (ii). But the left-hand side is a dth power, so each $\mathfrak{A}_i$ must be also. Using this fact and (iii) from above, write

$$\mathfrak{A}_i = \mathfrak{E}_i^d \qquad \text{and} \qquad \mathfrak{B}_i = \mathfrak{B}_i^*\mathfrak{Q}_i^d.$$

Then

$$\langle x-\alpha_i\rangle = \mathfrak{B}_i^*(\mathfrak{Q}_i\mathfrak{E}_i)^d\ ,$$

and we noted that there are only finitely many possibilities for the $\mathfrak{B}_i^*$. By (iv), we may write

$$\mathfrak{Q}_i\mathfrak{E}_i = \mathfrak{D}_{j_i}\langle z_i\rangle$$

with $z_i \in \mathfrak{O}_S$. Taking dth powers and noting that $\langle x-\alpha_i\rangle$ is a principal ideal in $\mathfrak{O}_S$, we have

$$\langle x-\alpha_i\rangle = \langle\xi_i\rangle\langle z_i^d\rangle,$$

with only finitely many possibilities for the principal ideal $\langle\xi_i\rangle$. Then

$$x-\alpha_i = u_i\xi_i z_i^d,$$

where $u_i \in U_S$, and ξ_i lies in a finite set. By observation (i), we have

$$u_i = \zeta_{k_i}\ u_i'^d,$$

with only finitely many possibilities for ζ_{k_i}. So finally, we get

$$x-\alpha_i = (\zeta_{k_i}\xi_i)(u_i'z_i)^d,$$

which gives the result with $\beta_i = \zeta_{k_i}\xi_i$ and $y_i = u_i'z_i$.

We return to the proof of Theorem 4A, considering two cases.

In the first case, we suppose $d \geqq 3,\ n \geqq 2$. Using the lemma, write

$$x-\alpha_1 = \beta_1 y_1^d,$$

$$x-\alpha_2 = \beta_2 y_2^d.$$

Then

$$\beta_1 y_1^d - \beta_2 y_2^d = \alpha_2-\alpha_1 \neq 0,$$

which is a Thue equation in the variables $y_1,\ y_2$ since $d \geqq 3$. So we have only finitely many solutions y_1, y_2. Since x is determined by the β_i's and y_i's, we have only finitely many possibilites for x.

The remaining case is when $d = 2$ and $n \geqq 3$. As above, write

$$x - \alpha_1 = \beta_1 y_1^2,$$

$$x - \alpha_2 = \beta_2 y_2^2,$$

$$x - \alpha_3 = \beta_3 y_3^2.$$

We need to solve this system of equations in $x, y_1, y_2, y_3 \in \mathfrak{O}_S$.

First, we extend K so that it contains $\sqrt{\beta}_1$, $\sqrt{\beta}_2$, $\sqrt{\beta}_3$. Then the right-hand sides will be squares, i.e., let $z_i = \sqrt{\beta}_i\ y_i$ so that $x - \alpha_i = z_i^2$ $(i = 1, 2, 3)$. Letting $\gamma_3 = \alpha_2 - \alpha_1 \neq 0$, and permuting the indices to get γ_1, γ_2, we have

$$z_1^2 - z_2^2 = \gamma_3,$$

$$z_2^2 - z_3^2 = \gamma_1,$$

$$z_3^2 - z_1^2 = \gamma_2.$$

Now the left-hand sides can be factored. We have, for instance,

$$(z_1 - z_2)(z_1 + z_2) = \gamma_3.$$

We write

$$z_1 - z_2 = \rho_3 u_3, \tag{4.2}$$

where u_3 is a unit and (since $z_1 - z_2$ divides γ_3) where we may take ρ_3 from a finite set. We also have

$$z_2 - z_3 = \rho_1 u_1,$$
$$z_3 - z_1 = \rho_2 u_2.$$

Adding these last three equations gives

$$\rho_1 u_1 + \rho_2 u_2 + \rho_3 u_3 = 0,$$

an S-unit equation. Hence there are only finitely many solutions $(u_1, u_2, u_3) \in \mathbb{P}^2(U_S)$.

We would like to know that there are only finitely many possibilities for the z_i $(i = 1, 2, 3)$. Then it will follow that there are only finitely many solutions to the original hyperelliptic equation in this case. So we consider

$$z_1 + z_2 = \frac{\gamma_3}{\rho_3 u_3}\ , \tag{4.3}$$

which in conjunction with (4.2) gives

$$z_1 = \frac{1}{2}\left(\rho_3 u_3 + \frac{\gamma_3}{\rho_3 u_3}\right)\ .$$

Similarly, by cyclic permutation,

$$z_2 = \frac{1}{2}\left(\rho_1 u_1 + \frac{\gamma_1}{\rho_1 u_1}\right)$$

and

$$z_3 = \frac{1}{2}\left(\rho_2 u_2 + \frac{\gamma_2}{\rho_2 u_2}\right).$$

We also have directly from (4.2), (4.3) that

$$z_2 = \frac{1}{2}\left(\frac{\gamma_3}{\rho_3 u_3} - \rho_3 u_3\right).$$

Now the γ_i are fixed and we have only finitely many choices for the ρ_i. There are finitely many possibilities for (u_1, u_2, u_3) up to equivalence in $\mathbb{P}^2(U_S)$. So suppose that we replace u_i by λu_i $(i = 1, 2, 3)$. Equating the two expressions for z_2 gives

$$(\rho_1 u_1 + \rho_3 u_3)\lambda = -\left(\frac{\gamma_1}{\rho_1 u_1} - \frac{\gamma_3}{\rho_3 u_3}\right)\frac{1}{\lambda},$$

so λ is determined (up to ±) unless $\rho_1 u_1 + \rho_3 u_3 = 0$, which is impossible.

In the next section, we will obtain estimates on the number of solutions.

§5. The Number of Solutions of Elliptic, Hyperelliptic, and Superelliptic Equations.

Here we discuss relatively explicit bounds on the number of solutions of the various equations. These results are the joint work of Evertse and Silverman (1986).

Let K be a number field of degree δ and $K^\times$ the multiplicative group of K. Let S be a finite set of absolute values which contains all of the non-Archimedean ones, i.e. $M_\infty(K) \subset S \subset M(K)$, and let $s = \operatorname{card} S$. As above, let $\mathfrak{O}_S$ denote the S-integers in K and U_S the S-units. Consider polynomials $f(X) \in \mathfrak{O}_S[X]$ with discriminant $\Delta(f) \in U_S$. Notice that this last requirement is not much of a restriction, since we may enlarge S to force $\Delta(f) \in U_S$. Then the cardinality s will reflect the number of prime factors of $\Delta(f)$.

In what follows, L is an extension of K with degree $[L : K] = \ell$. We will also have $d \geqq 2$, and $h_d(L)$ will denote the order of the subgroup of the ideal class group of L consisting of elements $[\mathfrak{A}]$ with $[\mathfrak{A}]^d = 1$. We will count solutions of the superelliptic equation

$$y^d = f(x), \tag{5.1}$$

with $x \in \mathfrak{O}_S$, $y \neq 0$, $y \in K$. (Then automatically, $y \in \mathfrak{O}_S$).

THEOREM 5A.

(a) *Suppose $d \geqq 3$, $n \geqq 2$, and L contains at least two roots of f. Then the number of solutions of (5.1) with $x \in \mathfrak{O}_S$ and $y \in K^*$ is*

$$\leqq 17^{\ell(6\delta+s)}\, d^{2\ell s}\, h_d(L).$$

(b) *Suppose $d = 2$, $n \geqq 3$ and L contains at least three roots of f. Then the number of solutions is*

$$\leqq 7^{\ell(4\delta+9s)}\, h_2(L)^2.$$

Remark. We may pick L with $\ell \leqq n(n-1)$ in case (a) and $\ell \leqq n(n-1)(n-2)$ in case (b). Aside from the choice of L, the coefficients of the polynomial f do not enter into the estimates. In the case of an elliptic equation, one may conclude that the number of solutions is $< c(\varepsilon)H^{2+\varepsilon}$, where H is the height of the equation. See Schmidt (to appear).

Here we will prove a weaker form of the case (a). We will show that the number of solutions in (a) is

$$\leqq (c_1 d)^{2\ell s}\ h_d(L).$$

We need several lemmas first.

LEMMA 5B. *Suppose* $|\ \ |$ *is a non-Archimedean absolute value on a field* E. *Let the polynomial*

$$f(X) = a_n X^n + \ldots + a_0 = a(X-\alpha_1)\ldots(X-\alpha_n),$$

be given with a_i, α_i *in* E *and* $|a_i| \leqq 1 \quad (i = 0, \ldots, n)$, *and also* $|\Delta(f)| = 1$ *where* Δ *denotes the discriminant. Then for every* $x \in E$ *with* $|x| \leqq 1$ *and* $i \neq j$, *we have*

$$\begin{aligned}|\alpha_i - \alpha_j| &= \max(|x-\alpha_i|,\ |x-\alpha_j|)\\ &= \max(1,\ |\alpha_i|)\ \max(1,\ |\alpha_j|).\end{aligned}$$

Proof. Because $|\ \ |$ is non-Archimedean, we have

$$\begin{aligned}|\alpha_i - \alpha_j| &\leqq \max(|x-\alpha_i|,\ |x-\alpha_j|)\\ &\leqq \max(1,\ |\alpha_i|)\ \max(1,\ |\alpha_j|).\end{aligned} \tag{5.2}$$

We also know that

$$|\Delta(f)| = |a_n|^{2n-2} \prod_{i\neq j} |\alpha_i - \alpha_j| = 1. \tag{5.3}$$

By Gauss' Lemma (and with the notation $|f| = \max\limits_i |a_i|$)

$$|a_n| \prod_{i=1}^{n} \max(1,\ |\alpha_i|) = |f| \leqq 1,$$

so

$$|a_n|^{2n-2} \prod_{i\neq j} \max(1,\ |\alpha_i|)\ \max(1,\ |\alpha_j|) \leqq 1. \tag{5.4}$$

Comparing (5.3) and (5.4) gives

$$\prod_{i\neq j} \max(1,\ |\alpha_i|) \max(1,\ |\alpha_j|) \leqq \prod_{i\neq j} |\alpha_i - \alpha_j|,$$

and this is

$$\leqq \prod_{i\neq j} \max(1,\ |\alpha_i|)\ \max(1,\ |\alpha_j|)$$

by (5.2). We therefore have equality everywhere, in particular in (5.2).

Now let $v \in M(K)$ such that $v \mid p$ for a prime p. Then v extends the p-adic absolute value. In this case, the value group G_v of v consists of powers π^ℓ ($\ell \in \mathbb{Z}$), where π is some fixed fractional power of p, say $\pi = p^{1/e}$.

LEMMA 5C. *Let v, π be as above. Suppose $|x|_v \leqq 1$, $|f|_v \leqq 1$, $|\Delta(f)|_v = 1$, and $f(x) = y^d$, where $y \in K^\times$. Then*

$$|x - \alpha_i|_v = \max(1,\ |\alpha_i|_v)\ \pi^{u_i d}\ ,$$

where $u_i \in \mathbb{Z}$ ($i = 1, \dots, n$). In fact, $u_i = 0$ with the possible exception of one value u_{i_0}.

Proof. By the proof of the preceding lemma, we have

$$|a_n|_v \prod_{i=1}^{n} \max(1,\ |\alpha_i|_v) = |f|_v = 1.$$

Since $f(x) \in (K^\times)^d$,

$$|f(x)|_v = |a_n|_v \prod_{i=1}^{n} |x - \alpha_i|_v \in G_v^d.$$

Then

$$\prod_{i=1}^{n} \frac{|x - \alpha_i|_v}{\max(1,\ |\alpha_i|_v)} \in G_v^d\ .$$

Letting $c_i = |x - \alpha_i|_v / \max(1,\ |\alpha_i|_v)$, we have

$$\prod_{i=1}^{n} c_i \in G_v^d\ .$$

Now if $|\alpha_i|_v > 1$, then $c_i = 1$. If, on the other hand, $|\alpha_i|_v \leqq 1$ and $|\alpha_j|_v \leqq 1$, then $|(x - \alpha_i) - (x - \alpha_j)\ |_v = |\alpha_i - \alpha_j|_v = 1$ by Lemma 5B. So only one of $|x - \alpha_i|$, $|x - \alpha_j|$ can be strictly less than 1, thus only one of c_i, c_j can be strictly less than 1. Therefore, $c_i = 1$ with one possible exception, and each $c_i \in G_v^d$. That is,

$$\frac{|x - \alpha_i|_v}{\max(1,\ |\alpha_i|_v)} \in G_v^d\,, \qquad (i = 1, \dots, n)$$

as desired.

As in Chapter III, Section 13, suppose there are t non-Archimedean elements of S. These absolute values correspond to prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_t$. Given fractional ideals $\mathfrak{A}, \mathfrak{B}$, we write

$$\mathfrak{A} \equiv \mathfrak{B}\,(\mathrm{mod}\, S)$$

if $\mathfrak{A}/\mathfrak{B}$ is of the type $\mathfrak{P}_1^{c_1} \dots \mathfrak{P}_t^{c_t}$ with integers $c_1, \dots, c_t$. We write $\mathfrak{A} \equiv \mathfrak{B} \,(\operatorname{mod} S, d)$ if $\mathfrak{A}/\mathfrak{B}$ is of the type $\mathfrak{P}_1^{c_1} \dots \mathfrak{P}_t^{c_t} \mathfrak{C}^d$ where $\mathfrak{C}$ is any fractional ideal. Consider the congruence in the variable z given by

$$\langle z \rangle \equiv \mathfrak{A} \,(\operatorname{mod} S, d) \qquad (5.4),$$

where $\langle z \rangle$ is the principal ideal with generator z. If z is a solution and $z' = zw^d$, then z' is also a solution. So it is valid to count solutions $z \in K^\times/(K^\times)^d$.

LEMMA 5D. *The number of solutions of the congruence (5.4) in $K^\times/(K^\times)^d$ is*

$$\leqq d^t \, h_d(K).$$

Proof. Suppose that there exists a solution z_0. Then for any other solution z, we have

$$\langle z/z_0 \rangle \equiv \langle 1 \rangle \ (\operatorname{mod} S,\ d).$$

Thus, it suffices to count solutions z of

$$\langle z \rangle \equiv \langle 1 \rangle \ (\operatorname{mod} S,\ d).$$

Suppose z is such a solution. By the definition of the congruence relation, we have

$$\langle z \rangle = \mathfrak{P}_1^{c_1} \dots \mathfrak{P}_t^{c_t} \mathfrak{C}^d,$$

and without a loss of generality, $0 \leqq c_i < d \quad (i = 1, \dots, t)$.

We will count solutions z with fixed $c_1, \dots, c_t$. Say z_1 is a fixed such solution,

$$\langle z_1 \rangle = \mathfrak{P}_1^{c_1} \dots \mathfrak{P}_t^{c_t} \mathfrak{C}_1^d$$

and z is an arbitrary such solution,

$$\langle z \rangle = \mathfrak{P}_1^{c_1} \dots \mathfrak{P}_t^{c_t} \mathfrak{C}^d \ .$$

Then

$$\langle z/z_1 \rangle = (\mathfrak{C}/\mathfrak{C}_1)^d \ .$$

The ideal class of $\mathfrak{C}/\mathfrak{C}_1$, say $[\mathfrak{C}/\mathfrak{C}_1]$, has $[\mathfrak{C}/\mathfrak{C}_1]^d = [1]$. Also, if $\mathfrak{C}, \mathfrak{C}_1$ are in the same ideal class, then $(z/z_1) \in (K^\times)^d$. So (since we only want solutions modulo $(K^\times)^d$) all that remains is to count ideal classes whose d th power is $[1]$. But their number is $h_d(K)$ by definition.

Allowing for all the possibilities for $c_1, \dots, c_t$ with $0 \leqq c_i < d \quad (i = 1, \dots, t)$, we have

$$\leqq d^t \, h_d(K)$$

solutions in $K^\times/(K^\times)^d$.

LEMMA 5E. *Suppose that $d \geqq 3$ and $\mathfrak{A}$ is a fractional ideal. Consider solutions $a \in K^\times$ to the pair of congruences*

$$\langle a \rangle \equiv \mathfrak{A} \,(\operatorname{mod} S, d),$$
$$\langle 1-a \rangle \equiv \langle 1, a \rangle \;(\operatorname{mod} S).$$

The number of such a is

$$\leqq (c_1 d)^{2s}\, h_d(K),$$

where c_1 is an absolute constant.

Proof. Write $a = wz^d$, where w runs through a complete residue system in $K^\times/(K^\times)^d$. Then by hypothesis,

$$\frac{\langle 1 - wz^d \rangle}{\langle 1,\; wz^d \rangle} \equiv \langle 1 \rangle \;\langle \operatorname{mod} S \rangle,$$

which may be written as

$$\frac{\langle 1 - \; wz^d \rangle}{\langle 1, wz^d \rangle} = \mathfrak{P}_1^{c_1} \ldots \mathfrak{P}_t^{c_t}.$$

For a given w, we count the number of solutions z. By Theorem 13E of Chapter III, the number of solutions is $\leqq (c_1 d)^s$ where c_1 is absolute. (Sorry about the occurrence of c_1 with two meanings.)

But we also have

$$\langle w \rangle \equiv \mathfrak{A} \,(\operatorname{mod} S, d),$$

where $w \in K^\times/(K^\times)^d$, and by the preceding lemma, the number of such w is $\leqq d^t\, h_d(K)$. Therefore, the total number of solutions is

$$\leqq (c_1 d)^{2s}\, h_d(K)\ .$$

We are now ready to return to the proof of Theorem 5A, part (a). We are considering solutions of the hyperelliptic equation

$$y^d = f(x) = a(x-\alpha_1)\ldots(x-\alpha_n),$$

where $x \in \mathfrak{O}_S, \quad y \in K^\times$.

In (a) we had $d \geqq 3$, $n \geqq 2$, and L contained at least two roots of f, say $\alpha_1, \alpha_2 \in L$. Let S' be the set of absolute values of L which extend absolute values of S.

For $x \in \mathfrak{O}_S$, put

$$Z(x) = \frac{x-\alpha_1}{x-\alpha_2}.$$

For $v \notin S'$, we have $|\Delta(f)|_v = 1$, so by Lemma 5B, we have

$$|\alpha_1 - \alpha_2|_v = \max\left(|x-\alpha_1|_v,\; |x-\alpha_2|_v\right)$$

and

$$\left|1-\frac{x-\alpha_1}{x-\alpha_2}\right|_v = \left|\frac{\alpha_1-\alpha_2}{x-\alpha_2}\right|_v = \max\left(1,\ \frac{|x-\alpha_1|_v}{|x-\alpha_2|_v}\right).$$

This means that for every $v \notin S'$

$$|1-Z(x)|_v = \max(1, |Z(x)|_v),$$

or in terms of prime ideals,

$$\langle 1-Z(x)\rangle \equiv \langle 1,\ Z(x)\rangle \ (\operatorname{mod} S').$$

Also, by Lemma 5C, for $v \in S'$, we have

$$\frac{|x-\alpha_i|_v}{\max(1,\ |\alpha_i|_v)} \in G_v^d \qquad (i=1,2),$$

so that

$$|Z(x)|_v = \frac{\max(1,\ |\alpha_1|_v)}{\max(1,\ |\alpha_2|_v)} \cdot g_v^d\ ,$$

with $g_v \in G_v$. Now we have

$$\langle Z(x)\rangle \equiv \mathfrak{A}(\operatorname{mod} S',\ d),$$

where $\mathfrak{A}$ is a certain ideal. By the last lemma, the number of possibilities for $Z(x)$ is $\leqq (c_1 d)^{2\ell s}\, h_d(L)$, since $\operatorname{card}(S') \leqq \ell \operatorname{card} S = \ell s$, where $\ell = [L:K]$.

§6. On Elliptic Curves.

Consider an irreducible polynomial equation

$$f(x,y)=0$$

and its associated affine curve, embedded in two-dimensional space. A point P on the curve is called a *singular* point if

$$\left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = 0.$$

Otherwise, it is called a *non-singular* point. For such a point, the equation of the tangent line at P is given by

$$\left(\left.\frac{\partial f}{\partial x}\right|_P\right)X + \left(\left.\frac{\partial f}{\partial y}\right|_P\right)Y = C\ ,$$

where C is a constant. Thus, at non-singular points, we have a well-defined tangent line.

If the total degree of f is d, then put

$$F(x,y,z)=z^d f\left(\frac{x}{z},\frac{y}{z}\right),$$

so that F is homogeneous of degree d. We study solutions of

$$F(x,y,z)=0,$$

where $(x,y,z)\in\mathbb{P}^2$. If the point (x_0,y_0) lies on the affine curve $F(x,y)=0$, then $(x_0,y_0,1)$ lies on the projective curve $F(x,y,z)=0$. Conversely, if (x_0,y_0,z_0) lies on the projective curve and $z_0\neq 0$, then $(x_0/z_0,\ y_0/z_0)$ lies on the affine curve. In other words, there is a one-to-one correspondence between points on the affine curve and points on the projective curve with $z\neq 0$. Points on the projective curve with $z=0$ are called the *points at infinity* of the affine curve. We say the curve is of degree d if F is of degree d.

Example. Consider $y^2=f(x)$, where f is a cubic with non-zero discriminant. We may write $y^2=a(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, and we see that the corresponding projective curve is $y^2z=a(x-\alpha_1z)(x-\alpha_2z)(x-\alpha_3z)$. The points at infinity occur when $z=0$, so $x=0$ and $y\neq 0$, i.e. the point $(0,1,0)\in\mathbb{P}^2$.

Example. Consider the cubic Thue equation $f(x,y)=m$ and the corresponding projective curve $f(x,y)=mz^3$. In factored form we have $a(x-\alpha_1y)(x-\alpha_2y)(x-\alpha_3y)=mz^3$. If $z=0$, then $x=\alpha_iy$ for some $i\in\{1,2,3\}$, so the three points at infinity are $(\alpha_1,1,0)$, $(\alpha_2,1,0)$, $(\alpha_3,1,0)\in\mathbb{P}^2$.

We will also need to talk about lines in projective space. Recall, a line in affine space is given by the equation $ax+by+c=0$, where a and b are not both zero. In projective space, this becomes $ax+by+cz=0$, where we require that a,b,c are not all zero. The additional line which appears, i.e. the line $z=0$, is called the *line at infinity*.

Recall, in affine space, we said the singular points on f correspond to

$$\frac{\partial f}{\partial x}(x,y)=\frac{\partial f}{\partial y}(x,y)=0 \quad\text{and}\quad f(x,y)=0\ .$$

In projective space, we have (recall that F was homogeneous of degree d)

$$dF(x,y,z)=\frac{x\partial F}{\partial x}(x,y,z)+\frac{y\partial F}{\partial y}(x,y,z)+\frac{z\partial F}{\partial z}(x,y,z)\ ,$$

so that singular points may reasonably be defined by

$$\frac{\partial F}{\partial x}(x,y,z)=\frac{\partial F}{\partial y}(x,y,z)=\frac{\partial F}{\partial z}(x,y,z)=0\ .$$

It is a simple lemma to prove that if an affine point is non-singular, then the corresponding projective point is also non-singular, and conversely.

Given a projective curve, we could specialize any of the variables to 1 to obtain corresponding affine curves. This is illustrated by the diagram here.

	affine curves
projective curve	$F(x,y,1)=0$
$F(x,y,z)=0$	$F(x,1,z)=0$
	$F(1,y,z)=0$

We may use these affine curves to study properties of the projective curve.

Example. Consider the curve $y^2 = f(x)$ with $\operatorname{discr}(f) \neq 0$. Does it contain any singular points? If so, there is a solution to $2y = 0$, $f(x) = 0$, $f'(x) = 0$, but this can not happen since $\operatorname{discr}(f) \neq 0$. What about the point at infinity? Is it a singular point? The projective curve is given by

$$y^2 z = a(x - \alpha_1 z)(x - \alpha_2 z)(x - \alpha_3 z)$$

and the point at infinity is $(0,1,0) \in \mathbb{P}^2$, as seen earlier. We check the partial with respect to z, and we see that

$$y^2 = \frac{\partial}{\partial z}\Big(a(x - \alpha_1 z)(x - \alpha_2 z)(x - \alpha_3 z)\Big)$$

which does not happen at $(0,1,0) \in \mathbb{P}^2$. So the curve is non-singular, i.e. it has no singular points.

Example. The projective cubic Thue equation $f(x,y) = mz^3$ is also non-singular.

Bezóut's Theorem. *If C_1, C_2 are projective curves of degrees d_1, d_2, respectively, then the total number of their intersection points (counted according to multiplicities which are not defined here) is $d_1 d_2$.*

In the special case of a cubic curve intersected with a line, the number of points of intersection is 3. Actually, it is not necessary to use the general version of Bezóut's Theoerem to get this result. We return to the examples once again, considering intersections with particular lines.

Example. Consider the cubic equation $y^2 = f(x)$ and the line at infinity, $z = 0$. Their intersection is the point $(0,1,0)$ in $\mathbb{P}^2$, so this point must have multiplicity 3.

Example. Consider the cubic $f(x,y) = mz^3$ where $f = a(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y)$ and the line $x = \alpha_i y$ for $i \in \{1,2,3\}$. These intersect at $(\alpha_i, 1, 0)$, which are all triple points of intersection.

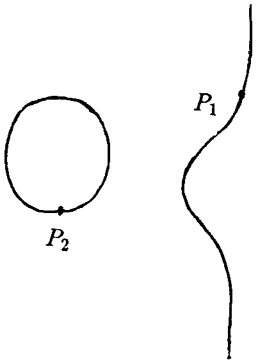
Now suppose that C is a non-singular curve. A *divisor* is a formal sum

$$D = \sum_{P \in C} c(P)P$$

where $c(P) \in \mathbb{Z}$ and $c(P) = 0$ for all but finitely many points P. The divisors of C form a group, denoted by Div C. For D a divisor, we let

$$\deg D = \sum_{P \in C} c(P).$$

Example.



For instance, $D = 3P_1 - 5P_2$ is a divisor with $\deg D = -2$.

Consider the affine line, i.e. the curve C which is the affine line. The rational functions on C are $r(x) = a(x)/b(x)$ where a, b are polynomials in x. At any $\alpha \in C$, we can expand $r(x)$ into a Laurent series, say

$$r(x) = \sum_{v=m}^{\infty} c_\nu (x - \alpha)^\nu$$

where (when $r \neq 0$) we may suppose that $c_m \neq 0$. We say $\text{ord}_\alpha r = m$. We put $\text{ord}_\alpha 0 = +\infty$.

Consider an affine curve C. A rational function on C is by definition a rational function $r(x, y) \in \mathbb{C}(x, y)$ whose denominator is not identically zero on C, with two functions r, s considered equal if they coincide on C.

Now consider a curve $C \subset \mathbb{P}^2$. We would like to define rational functions on C. They would have the form

$$r(x, y, z) = \frac{a(x, y, z)}{b(x, y, z)} ,$$

where a, b are homogeneous polynomials of equal degree and $b(x, y, z)$ is not identically zero on C. We will consider two rational functions on C as equal if they coincide for every point of C where their denominators are not zero.

Example. Consider the curve $y^2 = f(x)$. Then $r(P) = y$ is a rational function. We may rewrite r as

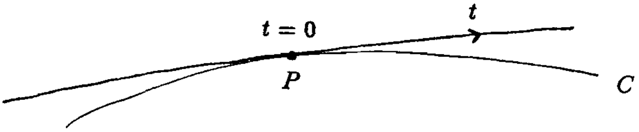
$$r(P) = y + y^2 - f(x).$$

If the curve is interpreted to lie in $\mathbb{P}^2$, then we may write

$$r(P) = \frac{y}{z} = \frac{yz^{d-1} + y^2 z^{d-2} - f(x/z) z^d}{z^d}$$

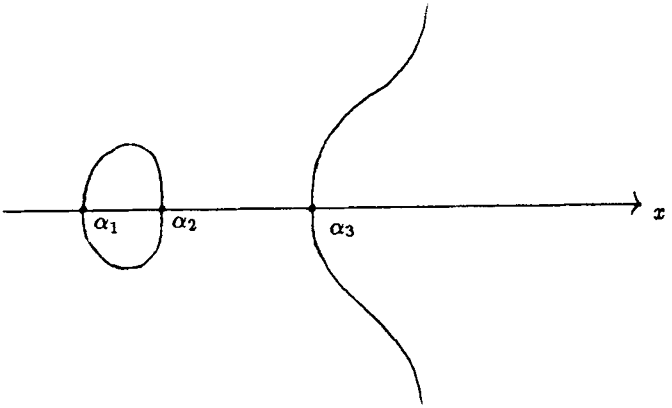
where $d = \deg f$.

Now suppose that r is some rational function on C and P is a point on C. If P is non-singular, then there exists a tangent line to C at P. Near P, everything can be expressed as a function of a *local parameter* t at P, as illustrated here.



For points on C near P, the function r may be written as a function of t, and r has a Laurent series in t. We let $\mathrm{ord}_P r$ denote the order of this Laurent series.

Example. We return to the curve $y^2 = f(x) = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. If the α_i are real, then we could have the following picture.

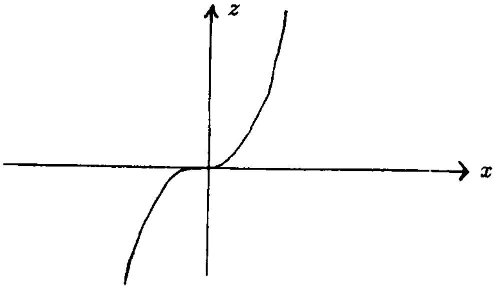


For P on C, take $r(P) = y$ as in the previous example. Then r vanishes only at $P_i = (\alpha_i, 0)$. Since the tangent lines are vertical, the local parameter is y itself, and $\mathrm{ord}_{P_i} r = 1 \quad (i = 1, 2, 3)$.

Example. Consider the above curve with $r(P) = x - \alpha_1$ for $P = (x, y)$. The function r vanishes at $P_1 = (\alpha_1, 0)$. There the local parameter is y. So we need to find the Laurent series for $x - \alpha_1$ in the variable y. We have $x - \alpha_1 = c_2 y^2 + c_4 y^4 + \dots$, and so $\mathrm{ord}_{P_1}(x - \alpha_1) = 2$.

So far, we have only considered $\mathrm{ord}_P r$ for non-singular *affine* points. By homogenizing the curve and the rational function r, we may consider non-singular projective points as well.

Example. Return to the curve $y^2 = f(x) = a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ and the rational function $r(P) = y$. We homogenize to $y^2 z = a(x - \alpha_1 z)(x - \alpha_2 z)(x - \alpha_3 z)$ and $r(P) = y/z$. Consider the point at infinity $P_\infty = (0, 1, 0)$. Then $\mathrm{ord}_{P_\infty}(y/z) = -\mathrm{ord}_{P_\infty}(z/y)$. We consider the affine curve with $y = 1$, that is, $z = a(x - \alpha_1 z)(x - \alpha_2 z)(x - \alpha_3 z)$, and the corresponding point at infinity $P_\infty = (0, 0)$. We can now determine ord$P_\infty(z)$. If $g(x,z)$ is the polynomial of this affine curve,then $\frac{\partial g}{\partial x} = 0$, $\frac{\partial g}{\partial z} = 1$ at P_∞.



So x is a local parameter, and we can expand $z = \gamma_3 x^3 + \ldots$. (See the figure above.) Then $\mathrm{ord}_{P_\infty} z = 3$ and $\mathrm{ord}_{P_\infty}(y/z) = -\mathrm{ord}_{P_\infty}(z) = -3$.

Combining this with what we saw above, we have

$$\mathrm{ord}_P y = \begin{cases} 1 & \text{if } P = P_i, \\ -3 & \text{if } P = P_\infty, \\ 0 & \text{everywhere else,} \end{cases}$$

and we see that

$$\sum_{P \in C} \mathrm{ord}_P y = 0 \ .$$

This is, in fact, true in general.

THEOREM. *If r is any non-zero rational function on a non-singular projective curve C, then*

$$\sum_{P \in C} \mathrm{ord}_P r = 0 \ .$$

This theorem will not be proved here. See e.g. Deuring (1973). Earlier, we had introduced the group of divisors, Div C, for a non-singular curve C. Given a non-zero rational function r on the curve C, we associate a divisor by

$$\mathrm{Div}\, r = \sum_{P \in C} (\mathrm{ord}_P r) P \ .$$

Then by the theorem, $\deg(\mathrm{Div}\, r) = 0$.

Example. For the curve $y^2 = f(x)$ and $r(P) = y$, as above, we have $\mathrm{Div}\, y = P_1 + P_2 + P_3 - 3P_\infty$.

A divisor D is called ***principal*** if $D = \mathrm{Div}\, r$ for some rational function r. We have $\mathrm{Div}(rs) = \mathrm{Div}(r) + \mathrm{Div}(s)$. We have the following inclusions.

$$\begin{array}{c} \text{group of divisors} \\ \cup| \\ \text{group of divisors of degree } 0 \\ \cup| \\ \text{group of principal divisors.} \end{array}$$

Now let D, E be two divisors on a non-singular curve C. Say

$$E = \sum_{P \in C} c^*(P)P \ ,$$

and D as above. We write $D \geqq E$ if $c(P) \geqq c^*(P)$ for every $P \in C$. This gives a partial ordering on the group of divisors. For a divisor D, we write $\mathfrak{L}(D)$ to denote the set of rational functions r with

$$\operatorname{Div} r \geqq -D.$$

Example. Let C be the x-axis and $P_1 = 1, P_2 = 2$. Let $D = 2P_1 - P_2$. Then $\mathfrak{L}(D)$ consists of all rational functions r with $\operatorname{Div} r \geqq -2P_1 + P_2$. This allows a pole of order at most 2 at P_1 and requires a zero of order at least 1 at P_2. Then, since no pole is allowed at ∞, $\mathfrak{L}(D)$ consists of all r of the form

$$\frac{(z-2)(az+b)}{(z-1)^2} \qquad (a, b \in \mathbb{C})$$

which shows that it is a vector space over $\mathbb{C}$ of dimension 2.

In general, $\mathfrak{L}(D)$ is a vector space over $\mathbb{C}$. We let $\ell(D) = \dim \mathfrak{L}(D)$. It is a consequence of the Riemann-Roch Theorem (see Deuring (1973)), there is a unique non-negative integer $g = g(C)$ such that if $\deg D > 2g - 2$, then $\ell(D) = (\deg D) - g + 1$. This g is called the *genus* of C, and it turns out to be the same as the topological genus which we mentioned earlier.

Example. Let C be the x-axis. Then it is easily seen that $g = 0$. For P_1, P_2 on C, let $D = 2P_1 - P_2$, so $\deg D = 1 > 2g - 2$. Then $\ell(D) = 1 - 0 + 1 = 2$, as we had determined earlier in a special case.

If D, E are divisors, we say $D \sim E$ if $D - E$ is a principal divisor. Notice that for D, E to be equivalent, it is necessary that $\deg D = \deg E$.

Example. Let C be the x-axis. If P, Q are any two points on C, then $(P) \sim (Q)$. For suppose that $P = \alpha$, $Q = \beta$, and both are finite. Then take $r(z) = (z - \alpha)/(z - \beta)$. Or if $P = \alpha$, $Q = \infty$, then take $r(z) = z - \alpha$.

In fact, for any curve C with $g = 0$, two points P, Q on C are equivalent. To see this, let $D = P - Q$. Then $\deg D = 0 > 2g - 2$, and we have $\ell(D) = 1$ by the consequence of the Riemann-Roch Theorem which was mentioned above. Hence there exists an f with $\operatorname{ord}_P f \geqq 1$, $\operatorname{ord}_Q f \geqq -1$, and $\operatorname{ord}_R f \geqq 0$ otherwise. Since $\sum_{R \in C} \operatorname{ord}_R f = 0$, the inequalities are all equalities. Then $D = \operatorname{Div} f$ and $(P) \sim (Q)$.

Now consider the case where $g = 1$. Take $D = (Q)$. Then $\deg D = 1 > 2g - 2$ and then $\ell(D) = 1$. Up to multiplication by $\mathbb{C}$, there exists one function r which has at most a pole at Q. In this case, $\mathfrak{L}(D)$ consists only of constants, so $(P) \sim (Q)$ is the same as $P = Q$.

LEMMA 6A. *Let C be a nonsingular curve with genus $g = 1$. Let O be a point on C. Given a divisor D with $\deg D = 0$, there is a unique $P \in C$ with*

$$(P) - (O) \sim D.$$

Proof. Let $D' = D + (O)$ so that $\deg D' = 1 > 0 = 2g - 2$. By the Riemann-Roch Theorem, $\ell(D') = \deg D' - g + 1 = 1$, so there exists a function f with $\mathrm{Div} f \geqq -D'$. Since $\deg \mathrm{Div} f = 0 = 1 - 1 = 1 + \deg(-D')$, there is a point P with $\mathrm{Div} f = -D' + (P) = -D - (O) + (P)$. But then $(P) - (O) \sim D$. The point P is unique, for if we had solutions P and P', then $(P) \sim (P')$ and thus $P = P'$ by previous work.

Let C be a nonsingular curve of genus 1, and let O be a point on C. Then C together with (O) is called an *elliptic curve.* Let $\mathfrak{D}_0$ be the group of divisors of degree 0 and $\mathfrak{D}_p$ the subgroup of principal divisors. By the preceding lemma, there is a $1 - 1$ correspondence between the points P on the curve and elements of the factor group $\mathfrak{D}_0/\mathfrak{D}_p$. (This factor group is called the Picard group). Namely, P corresponds to the class of $(P) - (O)$ modulus $\mathfrak{D}_p$. Since $\mathfrak{D}_0/\mathfrak{D}_p$ is a group, this induces a group structure on C. Let $P_1 + P_2$ be the sum of points, as defined in this way. Then

$$(P_1 + P_2) - (O) \sim (P_1) - (O) + (P_2) - (O).$$

Thus $P_1 + P_2$ is the unique point with

$$(P_1 + P_2) + (O) \sim (P_1) + (P_2).$$

The point O, which is called the *base point*, is the zero element of the group. Concerning the sum of n points, it is immediate that

$$(P_1 + \ldots + P_n) - (O) \sim (P_1) - (O) + \ldots + (P_n) - (O).$$

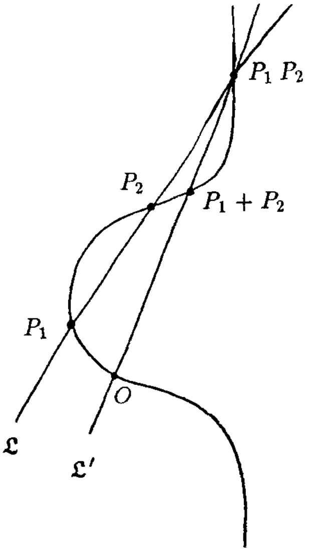
Our group law depends on the choice of the base point, but at any rate the group is isomorphic to $\mathfrak{D}_0/\mathfrak{D}_p$. Given points O, O', the canonical isomorphism g between the elliptic curves $C(O)$, $C(O')$ with respective base points O, O' is given by

$$(P) - (O) \longleftrightarrow (g(P)) - (O').$$

It may be shown that a nonsingular cubic curve has genus 1. Given a cubic curve C and two points P_1, P_2 on C, we would like to find a function f with

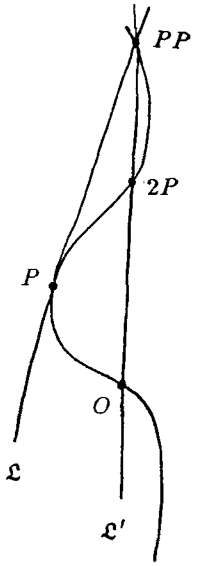
$$\mathrm{Div} f = (P_1 + P_2) + (O) - (P_1) - (P_2).$$

Then f has a zero of order 1 at $P_1 + P_2$ and 0 and poles of order 1 at P_1, P_2. For $P_1 \neq P_2$, we may have the following picture.

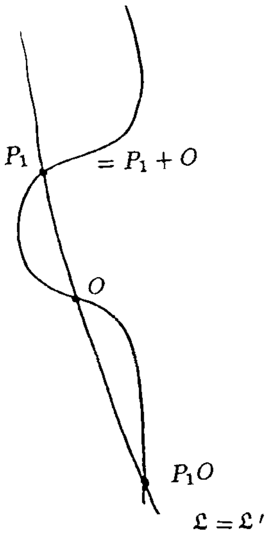


(Determine P_1P_2 as the point of intersection of C with the line $\mathfrak{L}$ through P_1, P_2. Then determine $\mathfrak{L}'$ as the line through O, P_1P_2. Finally $P_1 + P_2$ is the point of intersection of C and $\mathfrak{L}'$.) If $\mathfrak{L}$ is given by the linear form $L(\underline{\underline{x}}) = 0$ and $\mathfrak{L}'$ is given by $L'(\underline{\underline{x}}) = 0$, then $f(\underline{\underline{x}}) = L'(\underline{\underline{x}})/L(\underline{\underline{x}})$ has the desired properties.

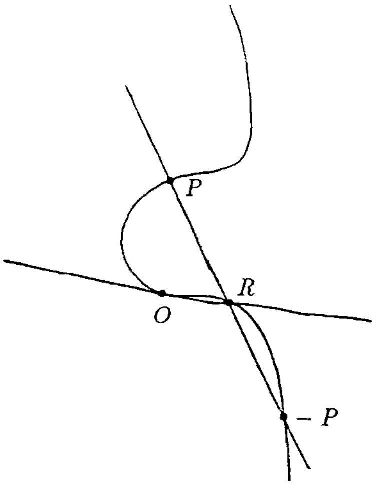
In the case where $P_1 = P_2$ ($= P$, say) we take $\mathfrak{L}$ to be the tangent line to C at P. Again we have $f(\underline{\underline{x}}) = L'(\underline{\underline{x}})/L(\underline{\underline{x}})$.



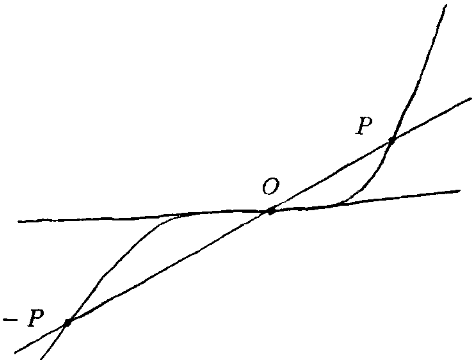
In the case where $P_2 = O$, take $\mathfrak{L} = \mathfrak{L}'$, and $f(\underline{x}) = 1$.



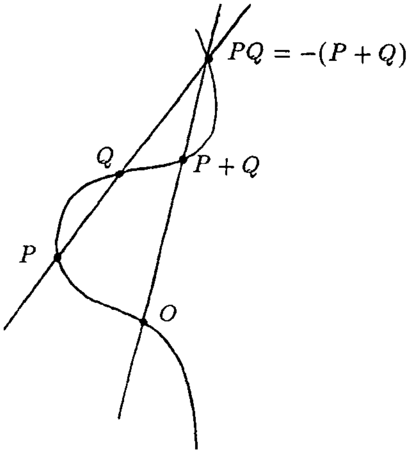
We may also use this graphical technique to find $-P$ for P on C. We draw the tangent line to C at the base point O. Call its third intersection point R. Then draw the line through P and R. Its third intersection point is $-P$. This is illustrated here.



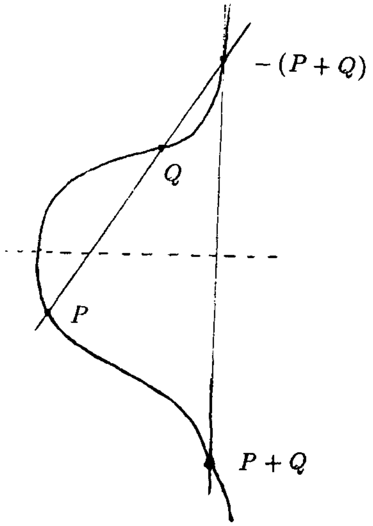
In the special case where O is a triple point on its tangent line, we have $O = R$ and the picture simplifies.



In this case we have another nice result. *We have $P + Q + S = O$ if and only if P, Q, S are colinear.*



Let $C : y^2 = f(x)$, where f is a cubic with distinct roots. Then we take $O = (0, 1, 0)$, which is a triple point of the line at infinity. Since the lines through this point at infinity are simply vertical lines, our picture looks like this.



Now suppose that our elliptic curve is a cubic of genus 1. Suppose also that it is defined by an equation with rational coefficients and that the base point O is rational. If P, Q are rational points on the curve then PQ is rational. Then, since O is rational, we have $P + Q$ rational. Thus given a rational point on our curve, we can generate other rational points.

Let $E(\mathbb{C})$ denote the group of all complex points on an elliptic curve E. Let $E(\mathbb{Q})$ denote the group of all rational points on E. Then $E(\mathbb{Q})$ is a subgroup of $E(\mathbb{C})$.

THEOREM (Mordell-Weil). *The group $E(\mathbb{Q})$ is finitely generated.*

The theorem as stated here is actually due to Mordell (1922), while Weil has generalized it. By the theorem, we know that

$$E(\mathbb{Q}) \simeq \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{\leftarrow r \text{ times} \rightarrow} \oplus \text{ Torsion},$$

where r is the *rank* of $E(\mathbb{Q})$, and the torsion part is finitely generated. Curves with rank as high as 14 are known. The conjecture is that there exist curves of arbitrarily large rank. There are, on the other hand, only finitely many possibilities for the torsion part.

THEOREM (Mazur). *There are exactly fourteen groups which may arise as the torsion part of an elliptic curve.*

Let $E \subseteq \mathbb{P}^2(\mathbb{Q})$ be an elliptic curve. Then every point on E may be represented as $(x(P), y(P), z(P))$, where $x(P), y(P), z(P) \in \mathbb{Z}$ are relatively prime. This representation is unique up to sign. The *Mordell-Weil height* is defined by

$$h_0(P) = \log(\max(|x(P)|,\ |y(P)|,\ |z(P)|)$$

The *Neron-Tate height* is given by

$$h(P) = \lim_{n \to \infty} \frac{h_0(2^n P)}{4^n}\ .$$

THEOREM. *The limit above exists, and $h(P) = 0$ if and only if P is a torsion point. If P is non-torsion, then*

$$h_0(P) \leqq c(E)h(P),$$

where $c(E)$ is a constant depending on E. Furthermore, $h(P)$ is a quadratic form on $E(\mathbb{Q})$, where a quadratic form is defined as below.

A *quadratic form* on an abelian group G is a real-valued function f such that for any P, Q in G we have

$$f(P+Q) + f(P-Q) = 2f(P) + 2f(Q)$$

The theorems generated in this section will not be proved here. For more on elliptic curves, see Silverman (1985).

Exercise 6a. Let $P_1, \ldots, P_k$ be in the abelian group G. Then

$$f(n_1P_1 + \ldots + n_kP_k) = \sum_{i,j=1}^{k} a_{ij}n_in_j,$$

where the coefficients a_{ij} depend on $P_1, \ldots, P_k$.

§7. The Rank of Cubic Thue Curves.

Consider the cubic Thue equation

$$F(x, y) = m,$$

where F is a homogeneous cubic polynomial in two variables with no multiple factors. The genus $g = 1$. This equation has the homogeneous form

$$F(x, y) = mz^3.$$

If the corresponding elliptic curve contains at least one rational point, then we can study the group of rational points $E_m(\mathbb{Q})$.

THEOREM 7A. *Given any such F, there is an integer $m_0 > 0$ such that rank $E_{m_0}(\mathbb{Q}) \geqq 1$.*

Our proof, which comes later, will follow the work of Silverman (1983).

PROPOSITION 7B. *The group of rational points on the curve $x^3 + y^3 = 657z^3$ has rank 3.*

This special result is not proven here. See tables compiled by Stephens (1968). The following result of Silverman (1983) shows that there exist Thue equations with rank at least 4.

PROPOSITION 7C. *For certain cubics F and certain values of m, we have*

$$\operatorname{rank} E_m(\mathbb{Q}) \geqq 4.$$

What about the torsion part of $E(\mathbb{C})$? Given a natural number n, there are n^2 points $P \in E(\mathbb{C})$ with $nP = O$.

LEMMA 7D. *Suppose $E(\mathbb{Q})$ is as above. Given any integer $d \geqq 1$, there are only finitely many points in $E(\mathbb{C})$ which are torsion points and whose coordinates generate an algebraic number field of degree no greater than d. In other words, the set*

$$\bigcup_{\substack{L \text{ number field} \\ [L:\mathbb{Q}] \leqq d}} E(L)_{\text{torsion}}$$

is finite.

The proof follows Silverman (1983), but first we need some preliminaries. Suppose $E(\mathbb{Q})$ and a prime p are given. By *reduction of the curve modulo p* we mean the following. Consider the corresponding equation $f(x, y) = 0$, which is an equation over $\mathbb{Z}$, and reduce the coefficients modulo p to obtain the new equation $\overline{f}(x, y) = 0$ over the finite field $\mathbb{F}_p$ with p elements. We say that we have a *good reduction* if the new curve is also an elliptic curve. In the previous section, we considered the equation $y^2 = f(x)$, where f was a cubic polynomial over $\mathbb{Z}$ with distinct roots. In this case if $\overline{\Delta f} \neq 0$, we have a good reduction. We also considered the cubic Thue equation $F(x, y) = m$, with certain restrictions on F. Here, if $\overline{\Delta F} \neq 0$ and $\overline{m} \neq 0$, we have a good reduction. In these cases, if p is a sufficiently large prime, we will get a good reduction. This is in fact true in general.

Now let $P = (x, y)$ be a rational point on E. If neither x nor y has a factor of p in its denominator, then consider $\overline{x}, \overline{y}$. We have $\overline{f}(\overline{x}, \overline{y}) = 0$. If p does occur in the denominator of either x or y, then homogenize the point P to get $(x, y, z) \in \mathbb{Z}^3$ with $gcd(x, y, z) = 1$. Then take the point $(\overline{x}, \overline{y}, \overline{z})$.

Example. Consider the equation $43x^3 - 2y^3 = 1$, the point $P = (1/3, 2/3)$, and the prime $p = 3$. Homogenize to get $P = (1, 2, 3)$ on the curve $43x^3 - 2y^3 = z^3$. Then $\overline{P} = (1, -1, 0)$ satisfies $x^3 + y^3 = z^3$.

Proof of Lemma 7D. Let $E(\mathbb{Q})$ and $d \geqq 1$ be given. Choose a prime p such that E has good reduction at p. Let L be any field with $[L : \mathbb{Q}] = d$, and choose a prime ideal $\mathfrak{P}$ of L lying above p. Take the curve $E(L)$ to be the set of all points on E with coordinates in L. Reduce this mod $\mathfrak{P}$ to get $E(\mathfrak{F}_{\mathfrak{P}})$, where $\mathfrak{F}_{\mathfrak{P}} = \mathfrak{O}/\mathfrak{P}$ is a finite field and $\mathfrak{O}$ is the ring of integers in L. From algebraic number theory, we have $\operatorname{card} \mathfrak{F}_{\mathfrak{P}} \leqq p^d$. So we have a map

$$E(L) \longrightarrow E(\mathfrak{F}_{\mathfrak{P}}),$$

where $E(\mathfrak{F}_{\mathfrak{P}})$ is the set of all points on the reduced curve with coordinates in $\mathfrak{F}_{\mathfrak{P}}$.

Now let $E(L)_p$ denote the "prime to p torsion" of $E(L)$ consisting of points P with the property that $mP = 0$ for some integer m with $p \nmid m$. Then the map

$$E(L)_p \longrightarrow E(\mathfrak{F}_{\mathfrak{P}})$$

is injective. (For a proof of this fact, see Silverman (1985, p.176).) We know that $E(\mathfrak{F}_{\mathfrak{P}}) \subset \mathbb{P}^2(\mathfrak{F}_{\mathfrak{P}})$, so we have

$$\operatorname{card}(E(\mathfrak{F}_{\mathfrak{P}})) \leqq (\operatorname{card} \mathfrak{F}_{\mathfrak{P}})^2 + (\operatorname{card} \mathfrak{F}_{\mathfrak{P}}) + 1.$$

Using the injective map above and the bound on $\operatorname{card}(\mathfrak{F}_{\mathfrak{P}})$ gives a bound

$$\operatorname{card} E(L)_p \leqq B(p, d, E).$$

Given another prime q with good reduction, we have

$$\operatorname{card} E(L)_q \leqq B(q, d, E).$$

But

$$\operatorname{Tor} E(L) \subseteq E(L)_p + E(L)_q,$$

so then

$$\operatorname{card}(\operatorname{Tor} E(L)) \leqq B(d, E).$$

Then for $P \in \operatorname{Tor} E(L)$, we have $mP = 0$ for some integer m with $m \leqq B(d, E)$. Here m may be different for each point P, but for fixed m, the number of such points P is no greater than m^2. So the total number of such points P, i.e. for any $m \leqq B(d, E)$, is

$$\leqq (B(d, E)!)^2,$$

and the result is proved.

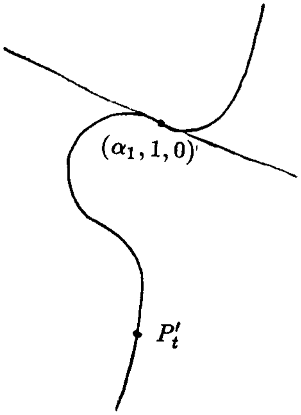
Before giving the proof of Theorem 7A, we state one further lemma.

LEMMA 7E. *Suppose $F(x, y) = mz^3$ is given where $F(x, y) = a(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y)$. The points $(\alpha_i, 1, 0)$ $(i = 1, 2, 3)$ are triple points on the curve.*

Proof. The lemma is true, since on the line $x = \alpha_i y$, the only point on the curve has $z = 0$.

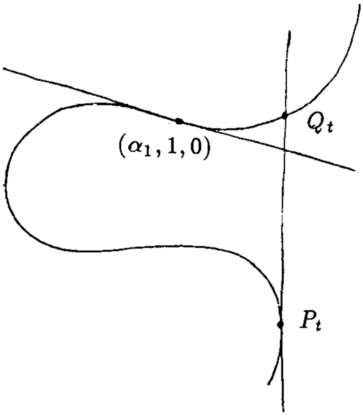
Proof of Theorem 7A. Given F, start with the curve

$$E: \ F(x, y) = z^3.$$



As illustrated, the point $P_t' = (t, 1, \sqrt[3]{F(t,1)})$, with $t \in \mathbb{Z}$, $\sqrt[3]{F(t,1)} \neq 0$ lies on E. Now take the new curve

$$E_t : \quad F(x,y) = F(t,1)z^3,$$



which contains the point $P_t = (t,1,1)$. We have a mapping

$$E \longrightarrow E_t : (x,y,z) \longmapsto (x,y,z/\sqrt[3]{F(t,1)}),$$

and it is a group isomorphism if $O = (\alpha_1, 1, 0)$ is the base point.

We consider E as a curve over $K = \mathbb{Q}(\alpha_1)$. Then P_t' has coordinates in a cubic extension of K. By Lemma 7D, for all but finitely many t, the point P_t' is non-torsion on E. So except for finitely many t, the point P_t is non-torsion on E_t.

Unfortunately, the base point O is not defined over $\mathbb{Q}$, but we want to consider $\operatorname{rank} E_m(\mathbb{Q})$, where $m = F(t,1)$. So we take P_t to be the new base point of E_t, and let Q_t be the third point of intersection of the tangent line to E_t at P_t. Now P_t, $Q_t \in E_t(\mathbb{Q})$, and with respect to this new base point, we claim that Q_t is non-torsion.

For suppose that Q_t were torsion with respect to the base P_t. Then $nQ_t = O$ for some integer n, which we write as an equivalence

$$n(Q_t) \sim n(P_t). \tag{7.1}$$

Since the original base point O is a triple point, we have $Q_t = -2P_t$, in the group operations with respect to base O. We write this as

$$(Q_t) + 2(P_t) \sim 3(O).$$

Then

$$n(Q_t) + 2n(P_t) \sim 3n(O). \tag{7.2}$$

Combining equivalences (7.1) and (7.2) gives

$$3n(P_t) \sim 3n(O),$$

so P_t is torsion with respect to the base O, a contradiction.

§8. Lower Bounds for the Number of Solutions of Cubic Thue Equations.

In (1933), Chowla studied equations of the form

$$x^3 - ky^3 = m.$$

Suppose $k \neq 0$ is given and let $Z(m)$ denote the number of solutions to the equation. Then Chowla proved that

$$Z(m) = \Omega_k(\log\log m)^{\dagger}$$

as $m \to \infty$. In other words,

$$Z(m) > c_k \log\log m$$

for infinitely many values of m. Mahler (1935) studied the more general cubic Thue equations

$$F(x,y) = m.$$

He showed that

$$Z_F(m) = \Omega_F((\log m)^{1/4}).$$

The latest result, which we state here, is due to Silverman (1983).

THEOREM 8A. *Suppose $F(x,y)$ is a form of degree 3 without multiple factors. Suppose there is some integer $m_0 \neq 0$ such that $F(x,y) = m_0$ has a rational solution and that the corresponding elliptic curve has Mordell-Weil rank $R > 0$. Then if $Z_F(m)$ is the number of solutions of $F(x,y) = m$, we have*

$$Z_F(m) = \Omega_F((\log m)^{R/(R+2)}).$$

In the preceding section, we showed (Theorem 7A) that there always exists an m_0 with rank $R \geqq 1$, which gives the following result.

COROLLARY 8B. *For any cubic form F as above, we have*

$$Z_F(m) = \Omega_F((\log m)^{1/3}).$$

COROLLARY 8C. *Suppose $F(x,y) = x^3 + y^3$. Then we can use $m_0 = 657$ and $R = 3$, so*

$$Z_F(m) = \Omega((\log m)^{3/5}).$$

COROLLARY 8D. *For certain cubic forms F, we can find m_0 with $R \geqq 4$, so*

$$Z_F(m) = \Omega_F((\log m)^{2/3}).$$

Corollaries 8C and 8D follow from Propositions 7B and 7C, respectively.

[†] Given $f(m), g(m) > 0$, we say $f(m) = \Omega(g(m))$ if there exists a constant $c > 0$ such that $f(m) > cg(m)$ for infinitely many values of m.

Remarks

(i) Nothing like this is known for $\deg F > 3$. It is quite possible that in this case there are bounds which are independent of m. It is also possible that Siegel's conjecture (Ch. III, first paragraph of §7) is true for curves of genus $g > 1$.

(ii) The function $Z_F(m)$ counts primitive as well as non-primitive solutions of $F(x,y) = m$. If $P_F(m)$ denotes the number of primitive solutions, then for all that we know, it is possible even in the cubic case that $P_F(m)$ is bounded independently of m.

(iii) The numbers m in the proof of the theorem will be of the type $m = m_0\ell^3$ where ℓ is large. It is conceivable that the number of solutions is bounded as m runs through cube-free integers.

Proof. Let E_0 be the curve given by the homogeneous equation

$$F(x,y) = m_0 z^3 \ .$$

For points P on E_0, write $(x(P), y(P), z(P))$, where $x(P), y(P), z(P)$ are co-prime integers. By hypothesis, this curve has Mordell-Weil rank $R > 0$. So there exist points $P_1, \dots, P_R$ on $E_0(\mathbb{Q})$ which generate a free abelian group of rank R. Let an integer $N \geqq 1$ be given and consider the set $\mathfrak{S}(N)$ of points

$$n_1P_1 + \dots + n_RP_R,$$

with

$$0 < n_i \leqq N \qquad (i = 1, \dots, R).$$

Then $\operatorname{card} \mathfrak{S}(N) = N^R$ and all of the points of $\mathfrak{S}(N)$ lie on the curve E_0.

If the base point O is chosen appropriately, then all of the non-torsion points P will have $z(P) \neq 0$. This is true if no root α_i of $F(x,1)$ is rational. If some root α_j is rational, then put $O = (\alpha_j, 1, 0)$, which is a triple point of intersection (of the curve and its tangent at O). Then if $z(P) = 0$, we have $f(x(P), y(P)) = 0$, and thus $x(P) = \alpha_i y(P)$ for some root α_i. Again P is a triple point of intersection. Then $3P = O$, a contradiction.

Now that we know $z(P) \neq 0$ for the non-torsion points, we put

$$m = m(N) = m_0 \prod_{P \in \mathfrak{S}\ (N)} z(P)^3. \tag{8.1}$$

We know that

$$F\left(\frac{x(P)}{z(P)}, \frac{y(P)}{z(P)}\right) = m_0$$

for $P \in \mathfrak{S}(N)$, and therefore

$$F\left(\frac{x(P)}{z(P)} \prod_{Q \in \mathfrak{S}\ (N)} z(Q),\ \frac{y(P)}{z(P)} \prod_{Q \in \mathfrak{S}\ (N)} z(Q)\right) = m_0 \prod_{Q \in \mathfrak{S}\ (N)} z(Q)^3 = m.$$

Therefore we have at least N^R integer solutions to $f(x,y) = m$.

Thus we need to obtain a lower bound for N^R in terms of m. For a non-torsion point $P = (x(P), y(P), z(P))$ we have

$$\begin{aligned}\log|z(P)| &\leqq h_0(P)\\ &= \log(\max(|x(P)|, |y(P)|, |z(P)|))\\ &\leqq ch(P),\end{aligned}$$

where $h_0(P)$ is the Mordell-Weil height and $h(P)$ is the Neron-Tate height. Notice that the last inequality holds since P is non-torsion. For the point $P = n_1P_1 + \ldots + n_RP_R$, we have

$$\begin{aligned}\log|z(P)| &\leqq c\sum_{i,j=1}^{R} c_{ij}\, n_i\, n_j\\ &\leqq c^*(n_1^2 + \ldots + n_R^2)\\ &\leqq c^{**}N^2,\end{aligned}$$

since $h(P)$ is a positive definite quadratic form in $n_1, \ldots, n_R$. Here c and the c_{ij} may depend on $P_1, \ldots, P_R$, thus c^{**} may depend on these points as well. By the definition of m in (8.1), we also have

$$\begin{aligned}\log|m| &= \log|m_0| + 3\sum_{P\in\mathfrak{S}\ (N)} \log|z(P)|\\ &\leqq 3c^{**}N^{R+2} + \log|m_0|.\end{aligned}$$

Combining this with our previous estimate for $Z_F(m)$, we get

$$Z_F(m) \geqq N^R \geqq c^{***}(\log|m|)^{R/(R+2)},$$

as desired.

Remark. Since, as we have seen in Theorem 1C of Ch. III, the number of solutions of $|F(x,y)| \leqq m$ is of smaller order of magnitude than m, the average number of solutions of $F(x,y) = m$, as m varies, is zero.

§9. Upper Bounds for Rational Points on Certain Elliptic Equations in Terms of the Mordell-Weil Rank.

Consider the Neron-Tate height $h(P)$ of points $P \in E(\mathbb{Q})$. We remarked in section 6 that

(i) $h(P) > 0$ if and only if P is non-torsion
(ii) $h(P)$ is a quadratic form.

Suppose that Q is a torsion point. Then for any point P, and for $n, m \in \mathbb{Z}$,

$$h(nP + mQ) = an^2 + bnm + cm^2.$$

If $\ell Q = 0$ where ℓ is a positive integer, then $h(nP + m\ell Q) = h(nP)$, so that $bnm\ell + cm^2\ell^2 = 0$ for $m \in \mathbb{Z}$, and therefore $b = c = 0$. In particular, $h(P+Q) = h(P)$, or in other words, $h(P) = h(P')$ if $P - P'$ is a torsion point. Therefore $h(P)$ is defined on the factor group $E(\mathbb{Q})/\text{Torsion}$.

Say rank $E(\mathbb{Q}) = R$ and

$$E(\mathbb{Q}) = \mathbb{Z}P_1 \oplus \ldots \oplus \mathbb{Z}P_R \oplus \text{Torsion}.$$

Then $h(n_1P_1 + \ldots + n_RP_R) = \sum_{i,j=1}^{n} a_{ij}\, n_i\, n_j$. By (ii), the quadratic form on the right here is positive if $n_1, \ldots, n_R$ lie in $\mathbb{Z}$ and are not all 0. In fact, it is known that this quadratic form is positive definite, i.e. it is positive if $n_1, \ldots, n_R$ lie in $\mathbb{R}$ and are not all 0. It is easily seen that this property does not depend on our choice of the base points $P_1, \ldots P_R$, and it is usually expressed by stating that

(iii) $h(P)$ is a positive definite quadratic form on $E(\mathbb{Q})/\text{Torsion}$.

A consequence is that

$$h(n_1P_1 + \ldots + n_RP_R) \geqq c_1(n_1^2 + \ldots + n_R^2)$$

where $c_1 > 0$. The number of integers $n_1, \ldots, n_R$ with $h(n_1P_1 + \ldots + n_RP_R) \leqq \xi$ is $\leqq c_2\, \xi^{R/2} + 1$. From Mazur's Theorem, card (Torsion) $\leqq 16$. As a consequence, *the number of points $P \in E(\mathbb{Q})$ with $h(P) \leqq \xi$ where $\xi \geqq 1$ is*

$$\leqq c_3(E)\, \xi^{R/2}.$$

Now we will consider elliptic equations of the form

$$y^2 = x^3 + D$$

and

$$E_{mD}: \qquad y^2 = x^3 + E_{mD},$$

where D is given and m varies. Recall that h_0 denotes the Mordell-Weil height.

THEOREM 9A. *Let $D \neq 0$ and $\xi \geqq 1$ be given. If $m \geqq m_0(D)$ and m is sixth power free, then the number of $P \in E_{mD}(\mathbb{Q})$ with*

$$h_0(P) < \xi \log m$$

is less than

$$16 \cdot (c_4\sqrt{\xi})^{\text{rank } E_{mD}(\mathbb{Q})},$$

where c_4 is an absolute constant.

In earlier sections, we used the Weierstrass type equation

$$y^2 = f(x),$$

where $f(x)$ is a cubic polynomial. Here it will be necessary to use the more general Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

It is easy to see that we may transform the second form into the first by the change of variables

$$y' = y + (a_1 x/2) + (a_3/2).$$

In general, transformations of the form

$$y = u^3 y' + u^2 s x' + t, \quad x = u^2 x' + r, \tag{9.1}$$

where $u \neq 0$, will transform a generalized Weierstrass equation into another equation of the same type. In fact, it can be shown that these are the only "rational" transformations with this property. We say that two Weierstrass equations over $\mathbb{Z}$ are *equivalent* if they are related by a transformation of the type (9.1).

Each general Weierstrass equation W is equivalent to a Weierstrass equation $y^2 = f(x)$. We then set

$$\Delta(W) = 16 \text{ discr.}(f);$$

it is easily shown that this quantity depends on W only.

If W has integral coefficients, f no longer necessarily does, but it may be shown that $\Delta(W)$ will be integral. Among all equivalent equations with integer coefficients we may pick one where $|\Delta(W)|$ is minimal. This discriminant is called $\Delta_{\min}$, and it may be associated with a Weierstrass equation of the more general form. One may check the algebra to see that $\Delta(W) = u^{12}\Delta(W')$ for W, W' related by a transformation as above. Thus if some $\Delta(W)$ is not divisible by any twelfth power, then we know that $\Delta_{\min} = \Delta(W)$.

Example. Consider our equation $y^2 = x^3 + D$. Then (see below) $\Delta = -16 \cdot 27D^2$. If $W : y^2 = x^3 + a^6 b$, then $\Delta(W) = -16 \cdot 27a^{12}b^2$. Now let $y = a^3 y'$, $x = a^2 x'$. Then we have $W' : y'^2 = x'^3 + b$, and $\Delta(W') = -16 \cdot 27b^2$.

LEMMA 9B. *Consider the curves*

$$E_D : \; y^2 = x^3 + D$$

and

$$E_{mD} : \; y^2 = x^3 + mD.$$

If m is sixth power free, then

$$\log \Delta_{\min}(E_{mD}) \geqq 2 \log |m| - 10 \log |6D|.$$

Proof. In the example, we said that

$$\Delta(E_D) = -16 \cdot 27 \, D^2 \, .$$

We may check this by considering the roots of $f(x) = x^3 + D$. They are $\alpha_1 = \alpha$, $\alpha_2 = \alpha\zeta$, $\alpha_3 = \alpha\zeta^2$, where $\alpha = \sqrt[3]{-D}$ and ζ is a primitive cube root of unity. Then

$$\begin{aligned}(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) &= \alpha^3(1-\zeta)(1-\zeta^2)(\zeta-\zeta^2)\\ &= -D(1-\zeta)^3(1+\zeta)\zeta\\ &= D(1-\zeta)^3\\ &= D(1-2\zeta+\zeta^2)(1-\zeta)\\ &= -D(3\zeta)(1-\zeta)\\ &= -3D(\zeta-\zeta^2)\\ &= -3D(2\zeta+1) = -3\sqrt{3}\,i\ D,\end{aligned}$$

since $\zeta = (-1+i\sqrt{3})/2$. Then $\operatorname{discr} f = -27D^2$. We also have

$$\Delta(E_{mD}) = -16\cdot 27m^2D^2.$$

For any transformation allowed, we would have $\Delta = \ell^{12}\Delta'$, where $\ell \in \mathbb{Q}^*$. So we get

$$-16\cdot 27m^2D^2 = \Delta(E_{mD}) = \ell^{12}\Delta_{\min}(E_{mD}).$$

Write $m = m_1m_2$, where m_1 is a product of primes p with $p \nmid 6D$ and m_2 is a product of primes p with $p \mid 6D$. Since m is sixth power free, we have

$$m_1^2 \mid \Delta_{\min}(E_{mD})$$

and

$$m_2 \leqq (6D)^5.$$

Then

$$\Delta_{\min}(E_{mD}) \geqq m_1^2\ ,$$

and the result follows by taking logarithms and applying the inequality for m_2.

LEMMA 9C. *Consider*

$$E_D:\ y^2 = x^3 + D.$$

If P is a non-torsion point on E_D, then

$$h(P) > c_5 \log \Delta_{\min}(E_D),$$

where $c_5 > 0$ is absolute.

This result is due to Silverman (1981). Lang has conjectured that the result is true for more general elliptic curves in Weierstrass form.

LEMMA 9D. *Let h_0 denote the Mordell-Weil height and h the Neron-Tate height. Then for P on a curve E in general Weierstrass form,*

$$|h(P) - h_0(P)| \leqq c_6 \log|\Delta(E)|.$$

This result is due to Zimmer (1976).

Proof. (of Theorem 9A.) Recall, we want to count the number of $P \in E_{mD}(\mathbb{Q})$ with

$$h_0(P) < \xi \log m,$$

where ξ and D are given. By Lemma 9D, we know that this is less than or equal to the number of $P \in E_{mD}(\mathbb{Q})$ having

$$h(P) < \xi \log m + c_6 \log \Delta(E_{mD}).$$

Write $P \in E(\mathbb{Q})$ as $P = P' + P''$ where $P'' \in$ Torsion and $P' = n_1P_1 + \ldots + n_RP_R$. By Mazur's Theorem, we have card(Torsion) $\leqq 16$. Combining this with Lemma 9B, we see that the number of P being counted is no greater than

$$16 \cdot \operatorname{card}\{P' \in E_{mD}(\mathbb{Q}) : h(P') < \xi \log m + 2c_6 \log m + c_7(D)\}.$$

Now we are back to a problem in the Geometry of Numbers. We know that $h(P')$ is a positive definite quadratic form F in R variables, and we need to count the number of points P' with $h(P') \leqq \nu = \xi \log m + 2c_6 \log m + c_7(D)$. We also have for nonzero P':

$$H(P') \geqq c_5 \log \Delta_{\min}(E_{mD}) = \nu_1,$$

say, by Lemma 9C. We use exercise 2b of Chapter I. Let $\mathcal{K}$ be the set of all $\underline{\underline{x}}$ with $F(\underline{\underline{x}}) \leqq 1$. We know that every integer point $\underline{\underline{x}} \neq \underline{\underline{0}}$ has $F(\underline{\underline{x}}) \geqq \nu_1$. So the first minimum λ_1 satisfies $\lambda_1 \geqq \sqrt{\nu_1}$. We count the number of points $\underline{\underline{x}}$ with $F(\underline{\underline{x}}) \leqq \nu$, i.e. the number of integer points in the set $\sqrt{\nu}\mathcal{K}$. By the exercise, the number of such points is

$$\leqq \left(2\sqrt{\frac{\nu}{\nu_1}} + 1\right)^R .$$

Since for $m \geqq m_0(D)$ we have $\nu \leqq (\xi + 2c_6 + 1) \log m \leqq c_8\, \xi\, \log m$, and $\nu_1 \geqq c_9 \log m$, we have $\sqrt{\nu/\nu_1} \leqq c_{10}\, \xi^{1/2}$, so that we obtain

$$\leqq (2c_{10}\, \xi^{1/2} + 1)^R \leqq (c_4\, \xi^{1/2})^R .$$

Theorem 9A follows.

§10. Isogenies.

Let C_1, C_2 be curves in $\mathbb{C}^2$. We want to discuss maps from C_1 to C_2. A *rational map* is a map given by rational functions ϕ, ψ on C_1 such that whenever $(x, y) \in C_1$ and ϕ, ψ are defined at (x, y), then $(\phi(x, y),\ \psi(x, y)) \in C_2$.

However, it is better to think of C_1, C_2 as curves in $\mathbb{P}^2$. Then we consider maps of the form

$$(x, y, z) \mapsto (\phi_1(x, y, z),\ \phi_2(x, y, z),\ \phi_3(x, y, z)),$$

where ϕ_1, ϕ_2, ϕ_3 are homogeneous polynomials of equal degree such that for $(x, y, z) \in C_1$ we don't have (ϕ_1, ϕ_2, ϕ_3) identically $(0,0,0)$, and we have $(\phi_1(x,y,z),\ \phi_2(x,y,z),\ \phi_3(x,y,z)) \in C_2$ whenever $(\phi_1, \phi_2, \phi_3) \neq (0,0,0)$. More precisely, we consider equivalence classes of such functions (ϕ_1, ϕ_2, ϕ_3). One says

$$(\phi_1, \phi_2, \phi_3) \sim (\phi_1', \phi_2', \phi_3')$$

if the matrix

$$\begin{pmatrix} \phi_1(\underline{\underline{x}}) & \phi_2(\underline{\underline{x}}) & \phi_3(\underline{\underline{x}}) \\ \phi_1'(\underline{\underline{x}}) & \phi_2'(\underline{\underline{x}}) & \phi_3'(\underline{\underline{x}}) \end{pmatrix}$$

has rank $\leqq 1$ for every $\underline{\underline{x}} \in C_1$.

Example. Let

$$C_1 : \mathbb{P}^1 \qquad \text{and} \qquad C_2 : x^2 + y^2 = 1.$$

The rational map

$$t \longmapsto \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$$

can be viewed as the map

$$(t, w) \longmapsto (2tw,\ t^2 - w^2,\ t^2 + w^2).$$

Example. Let

$$C_1 : x^4 + y^4 = 1 \qquad \text{and} \qquad C_2 : u^2 + v^2 = 1.$$

A map which takes C_1 into C_2 is

$$(x, y) \longmapsto (x^2, y^2) = (u, v).$$

A non-constant map has a *degree* δ which is defined as the largest integer such that δ points on C_1 are mapped into a single point on C_2. In the first example, one could find an inverse map, so $\delta = 1$. In the second example, $\delta = 4$.

Fact. If C_1, C_2 are non-singular curves in $\mathbb{P}^2$, then a rational map $C_1 \to C_2$ is necessarily defined everywhere. If C_1, C_2 are irreducible and the map $\underline{\underline{\phi}}$ is not constant, then $\underline{\underline{\phi}}$ is onto C_2. (See, e.g. Silverman (1985), Ch. II, Prop. 2.1 and Theorem 2.3).

An *isogeny* of elliptic curves E_1, E_2 with respective base points O_1, O_2 is defined as a non-constant rational map $\underline{\underline{\phi}} : E_1 \to E_2$ with $\underline{\underline{\phi}}(O_1) = O_2$. By what we just said above, such a map is onto.

THEOREM 10A. *An isogeny is a homomorphism of the groups belonging to E_1 and E_2.*

How would one begin to prove this? We have

$$(P+Q)+(O_1)\sim(P)+(Q),$$

where $\sim$ is an equivalence relation on the divisors of E_1. We would need

$$(\underline{\underline{\phi}}(P+Q))+(\underline{\underline{\phi}}(O_2))\sim(\underline{\underline{\phi}}(P))+(\underline{\underline{\phi}}(Q)),$$

where $\sim$ is now the equivalence relation on divisors of E_2. So we have a rational function f on E_1 such that

$$\operatorname{Div} f=(P)+(Q)-(O_1)-(P+Q),$$

and we need a rational function f_* on E_2 with

$$\operatorname{Div} f_*=(\underline{\underline{\phi}}(P))+(\underline{\underline{\phi}}(Q))-(\underline{\underline{\phi}}(O_2))-(\underline{\underline{\phi}}(P+Q)).$$

If

$$D=\sum_{i=1}^{\ell}c_i(P_i)$$

is a divisor of E_1, then let

$$\underline{\underline{\phi}}_*(D)=\sum_{i=1}^{\ell}c_i(\underline{\underline{\phi}}(P_i))$$

on E_2. So it would suffice if with every rational function f of E_1, we could associate a rational function $\underline{\underline{\phi}}_*(f)=f_*$ on E_2 such that

$$\operatorname{Div}(\underline{\underline{\phi}}_*(f))=\underline{\underline{\phi}}_*(\operatorname{Div} f).$$

It is proved in Algebraic Geometry that this can be done. (See Silverman (1985), Ch. II, Prop. 3.6).

Now suppose the functions defining $\underline{\underline{\phi}}:\ E_1\mapsto E_2$ have rational coefficients. Then

$$\underline{\underline{\phi}}:\ E_1(\mathbb{Q})\to E_2(\mathbb{Q}).$$

Since $\underline{\underline{\phi}}$ is a group homomorphism, it is precisely $\delta:1$ where δ is the degree, and the kernel is of order δ. It is a general fact that a homomorphism with finite kernel of free abelian groups preserves the rank.

Consider the special case of a binary cubic form

$$F(x,y)=ax^3+bx^2y+cxy^2+dy^3$$

with distinct linear factors. Take the curve

$$C_m:\ F(x,y)=m.$$

Exercise 10a. Consider binary cubic F forms with complex coefficients and non-zero discriminant along with non-singular linear maps $T:\ \mathbb{C}^2 \to \mathbb{C}^2$. Let $F_0(x,y) = x^3 + y^3$. Then any such F is of the form $F(\underline{\underline{x}}) = F_0(T(\underline{\underline{x}}))$ for a suitable T.

Given a binary cubic form

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3,$$

associate with it

$$\begin{aligned} G(x,y) &= \frac{1}{4}\begin{vmatrix} F_{xx} & F_{xy} \\ F_{yx} & F_{yy} \end{vmatrix} \\ &= (3ac - b^2)x^2 + (9ad - bc)xy + (3bd - c^2)y^2 \end{aligned}$$

and

$$\begin{aligned} H(x,y) &= \begin{vmatrix} F_x & F_y \\ G_x & G_y \end{vmatrix} \\ &= (27a^2d - 9abc + 2b^3)x^3 - 3(6ac^2 - b^2c - 9abd)x^2y \\ &+ 3(6b^2d - bc^2 - 9acd)xy^2 - (27ad^2 - 9bcd + 2c^3)y^3. \end{aligned}$$

The new forms G, H are called *covariant forms.* We also introduce the notation

$$F^T(\underline{\underline{x}}) = F(T(\underline{\underline{x}})).$$

If

$$F \longmapsto F^T,$$

then

$$G \longmapsto (\det T)^2 G^T$$

and

$$H \longmapsto (\det T)^3 H^T.$$

Remark. This is easy to check, using the two special transformations with matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

Consider the curve

$$J_m:\ y^2z = x^3 - 432m^2Dz^3,$$

where $D = \operatorname{discr} F$ and F is as above. We have a map

$$\underline{\underline{\phi}}:\ C_m \longmapsto J_m:\ (x,y,z) \to (-4zG(x,y),\ 4H(x,y), z^3).$$

To see that such $\underline{\underline{\phi}}$ really maps into J_m, look first at the special case where $m = 1$ and $F(x,y) = x^3 + y^3$. We have

$$\begin{aligned} C &: x^3 + y^3 = z^3 \\ J &: y^2z = x^3 - 432(-27)z^3, \end{aligned}$$

since $D = -27$. Then $F = F_0 = x^3 + y^3$ and $G = 9xy$ and $H = 27(x^3 - y^3)$. We need

$$16H^2z^3 = -64z^3G^3 + 432 \cdot 27z^9,$$

i.e. we need

$$H^2 = -4G^3 + 27^2z^6,$$

which does hold. The general truth follows, since we have $F = F_0^T$ in general and G, H have the necessary covariance properties.

Under this map, a point on C_m with $F(x,y) = 0$, $z = 0$ will be mapped onto $(0, 4H(x,y), 0) = (0,1,0)$ since $H(x,y) \neq 0$. Also, if C_m has any rational point, say O_1, then $\underline{\underline{\phi}}(O_1) = O_2$ will be rational on J_m. Now $\underline{\underline{\phi}}$ defines an isogeny from C_m with base point O_1 to J_m with base point O_2.

§11. Upper Bounds on Cubic Thue Equations in Terms of the Mordell-Weil Rank.

As in section 8, we consider curves of the type

$$C_m : \ F(x,y) = m,$$

where F is a form of degree 3 with no multiple factors. If C_m contains no rational points then we have a trivial upper bound. So suppose that C_m contains a rational point. Then we have an elliptic curve with some $R =$ rank $C_m(\mathbb{Q}) = R$, say.

THEOREM 11A. *When $m > m_0(F)$ and m is cube-free and C_m contains a rational point, then the number of integer solutions of the cubic Thue equation $F(x,y) = m$ is*

$$< c^{1+\text{rank } C_m(\mathbb{Q})},$$

where c is an absolute constant.

This result is due to Silverman (1982), but there was an earlier attempted proof by Demjanenko (1974). Recall that Bombieri and Schmidt have given the bound

$$c_0\, 3^{1+\nu},$$

where $\nu = \nu(m)$ is the number of distinct prime factors of m, and only the primitive solutions are counted. These two estimates are rather different and, at this point, no one has shown how they fit together. (See also C. Stewart (to appear)).

Suppose there exists some form F such that as m ranges over positive cube-free integers, then the number of solutions of $F(x,y) = m$ is unbounded as a function of m. If this is so, then rank $(C_m(\mathbb{Q}))$ is unbounded, and this would prove the conjectured existence of elliptic curves of arbitrarily high rank.

LEMMA 11B. *Consider the Thue equation*

$$F(x,y) = m$$

of degree 3 *and define*

$$H^*(F) = (\text{cont } F)\, h_K(\alpha_i)$$

as in Chapter III, Section 2. Then the number of solutions to this Thue equation with

$$\max(|x|,\, |y|) > 4^8 H^*(F)^8 m^{8/d}$$

is

$$\ll d.$$

Proof. By Lemma 3C of Chapter III, we have

$$\left|\alpha - \frac{x}{y}\right| < \frac{d}{2} \cdot 2^d \cdot \frac{h_K(\alpha)^{d-2} m}{|y|^d}$$

for some root α of $F(x,1)$. If $|y| \geqq |x|$, we get

$$\left|\alpha - \frac{x}{y}\right| < \frac{4^d H^*(F)^d m}{y^{d/8}\ y^{3\sqrt{d}/2}} < \frac{1}{y^{3\sqrt{d}/2}}\ .$$

By a result of Chapter III, the number of solutions of this last relation with $y \geqq H^*(F)$ is $\ll d$.

Now we are able to prove Theorem 11A. Suppose we have a solution $(x,y) \in \mathbb{Z}^2$ of $F(x,y) = m$. Then $(x,y,1)$ is a point on the curve $C_m :\ F(x,y) = mz^3$. As in the preceding section, we have a map $\underline{\underline{\phi}} :\ C_m \to J_m$, where $J_m :\ y^2 z = x^3 - 432m^2 D$. Let h_0 be the Mordell-Weil height on J_m. Then since $\underline{\underline{\phi}}$ was defined in terms of cubic forms,

$$h_0\left(\underline{\underline{\phi}}\,(x,y,1)\right) \leqq 3 \log |\underline{\underline{x}}| + c_1(F).$$

By the lemma above, we have

$$|\underline{\underline{x}}| \leqq 4^8\ H^*(F)^8 m^{8/3}$$

with $\leqq c_2$ exceptions. If $\underline{\underline{x}}$ is not an exception, then

$$h_0\left(\underline{\underline{\phi}}\,(x,y,1)\right) \leqq 8 \log m + c_3(F) \leqq 9 \log m$$

for $m \geqq c_4(F)$. We apply Theorem 9A with $-432D$ in place of D. Since m is sixth power free, the number of rational points P on J_m with $h_0(P) \leqq 9 \log m$ is

$$\leqq c_4^{1+\textbf{rank}\ J_m} = c_4^{1+\textbf{rank} C_m}$$

since J_m is obtained from C_m by an isogeny. Since $\underline{\underline{\phi}}$ is at most six to one, we get an estimate for the number of integer points on C_m.

§12. More general results. Our discussion would be incomplete without at least a mention of the following deep results. Their proofs, however, are beyond the scope of these Notes.

Siegel in (1929) proved that the number of integer points (x, y) of any irreducible curve

$$f(x,y) = 0 \tag{12.1}$$

of genus $g > 0$ is finite. Baker and Coates (1970), in the case $g = 1$, gave effective bounds for the number and the size of such points. They accomplished this by constructing a suitable birational transformation to an elliptic curve $y^2 = f(x)$. Better bounds were recently achieved by Schmidt (to appear): If (12.1) defines an irreducible curve of genus 1, where f has rational coefficients, then the number of integer solutions $x, y \in \mathbb{Z}$ is

$$< c_1(d) H^{c_2(d)},$$

where H is the height of f, where d is its degree, and $c_2(d)$ is a polynomial in d. (E.g., a polynomial of degree 13, but this can surely be improved. Furthermore, possible integer solutions have

$$\max\Big(|x|, |y|\Big) < \exp\Big(c_1(d) H^{c_2(d)}\Big).$$

Faltings (1983) proved Mordell's conjecture, that on a curve of genus $g > 1$, there are only finitely many <u>rational</u> points. Another proof, with ideas closer to diophantine approximations, was given by Vojta (to appear), with a more elementary version given by Bombieri (to appear). There is every hope that this will lead to bounds on the <u>number</u> of rational points. However, when $g > 1$, effective results on the size of integer points or rational points (the size of numerators and denominators) seem at present to be quite beyond reach.

V. Diophantine Equations in More than Two Variables.

References: Evertse, Györy, Stewart and Tijdeman (1988), Schmidt (1980)

§1. The Subspace Theorem.

THEOREM 1A. (Subspace Theorem, Schmidt (1972)). *Suppose that $L_1, \dots, L_n$ are linearly independent linear forms in n variables with algebraic coefficients. Suppose $\delta > 0$ is given. Then the integer points $\underline{\underline{x}} \neq \underline{\underline{0}}$ with*

$$|L_1(\underline{\underline{x}}) \dots L_n(\underline{\underline{x}})| < |\underline{\underline{x}}|^{-\delta}$$

lie in a finite number of proper subspaces of $\mathbb{Q}^n$.

The reader may find a proof in Schmidt (1980).

CORROLLARY 1B. *Suppose $\alpha_1, \dots, \alpha_n$ are algebraic and $1, \alpha_1, \dots, \alpha_n$ are linearly independent over $\mathbb{Q}$. Then there are only finitely many rational n-tuples $(x_1/y, \dots, x_n/y)$ with $y > 0$ and*

$$\left|\alpha_i - \frac{x_i}{y}\right| < \frac{1}{y^{1+(1/n)+\delta}}, \qquad (i = 1, \dots, n). \tag{9.1}$$

In the special case $n = 1$, we get Roth's Theoerem. Also, the exponent $1 + (1/n)$ is best possible by Dirichlet's Theorem (Theorem 1B of Chapter II).

Proof. Multiplying together all of the inequalities in (9.1), then multiplying by y^{n+1} gives

$$y|\alpha_1 y - x_1| \dots |\alpha_n y - x_n| < 1/y^\delta.$$

Now put $\underline{\underline{x}} = (x_1, \dots, x_n, y) \in \mathbb{Z}^{n+1}$ and let $\underline{\underline{X}} = (X_1, \dots, X_n, Y)$. Let

$$L_i(\underline{\underline{X}}) = \alpha_i Y - X_i \qquad (i = 1, \dots, n)$$

and

$$L_{n+1}(\underline{\underline{X}}) = Y.$$

Then we have

$$|L_1(\underline{\underline{x}}) \dots L_{n+1}(\underline{\underline{x}})| < 1/y^\delta < 1/|\underline{\underline{x}}|^{\delta/2}$$

if y is large.

By the Subspace Theorem in $n + 1$ dimensions, the solutions lie in a finite number of subspaces. Let one such subspace be given by

$$c_1 x_1 + \dots + c_n x_n + c_{n+1} y = 0$$

with $c_i \in \mathbb{Q}$. On this particular subspace we have

$$(c_1\alpha_1 + \dots + c_n\alpha_n + c_{n+1})y = c_1(\alpha_1 y - x_1) + \dots + c_n(\alpha_n y - x_n)$$

by the defining equation above. Let $\gamma = c_1\alpha_1 + \ldots + c_n\alpha_n + c_{n+1}$. Then $\gamma \neq 0$ by the linear independence of $1, \alpha_1, \ldots, \alpha_n$, and also γ is fixed for a given subspace. We have

$$\begin{aligned} |\gamma|\,|y| &\leqq (|c_1| + \ldots + |c_n|)/y^{(1/n)+\delta} \\ &\leqq |c_1| + \ldots + |c_n|. \end{aligned}$$

So y is bounded and we are finished.

One would like to make the Subspace Theorem more quantitative. Recall, Roth's Theorem is ineffective in the sense that it does not give estimates for x, y. It can be strengthened, as we have seen, to give bounds on the number of solutions. A similar result is true in this case as well. We can not estimate the coefficients of the defining equations of the subspaces (i.e., we cannot estimate their heights), but we can give a bound for the *number* of subspaces.

THEOREM 1C. (Schmidt (1989a)). *Let $L_1, \ldots, L_n$ be linearly independent linear forms with coefficients in an algebraic number field of degree d. Consider the inequality*

$$|L_1(\underline{\underline{x}}) \ldots L_n(\underline{\underline{x}})| < |\det(L_1, \ldots, L_n)|\,|\underline{\underline{x}}|^{-\delta},$$

where $0 < \delta < 1$. Then there are proper subspaces $S_1, \ldots, S_t$ of $\mathbb{Q}^n$ where

$$t = \left[(2d)^{2^{26n}\,\delta^{-2}}\right],$$

such that all integer solutions $\underline{\underline{x}} \neq \underline{\underline{0}}$ lie in the union of $S_1, \ldots, S_t$ and the ball

$$|\underline{\underline{x}}| \leqq \max((n!)^{8/\delta},\ H(L_1), \ldots, H(L_n)).$$

Schlickewei (1977) generalized Schmidt's Subspace Theorem to allow more general absolute values.

THEOREM 1D. *Let K be an algebraic number field and let $S \subset M(K)$ be a finite set of absolute values which contains all of the non-Archimedean ones. For $v \in S$, let $L_{v1}, \ldots, L_{vn}$ be n linearly independent linear forms in n variables with coefficients in K. Let $\delta > 0$ be given. Then the solutions of the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{vi}(\underline{\underline{x}})|_v^{n_v} < \overline{|\underline{\underline{x}}|}^{-\delta}$$

with $\underline{\underline{x}} \in \mathfrak{O}_K^n$ and $\underline{\underline{x}} \neq \underline{\underline{0}}$, where

$$\overline{|\underline{\underline{x}}|} = \max_{\substack{1 \leqq i \leqq n \\ 1 \leqq j \leqq \deg K}} |x_i^{(j)}|,$$

lie in finitely many proper subspaces of K^n. (As always, $\mathfrak{O}_K$ is the ring of integers in K, and n_v is the local degree).

A quantitative result was proved by Schlickewei, (to appear (a). See also (b).)

THEOREM 1E. *Let $S \subset M(\mathbb{Q})$ be of finite cardinality s, and containing the Archimedean absolute value. Let K be a number field of degree d, and suppose that for each $v \in S$ we are given a fixed extension of $|\cdot|$ to K. For $v \in S$, let $L_{v1}, \dots, L_{vn}$ be n linearly independent linear forms in n variables and with coefficients in K. Consider the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{vi}(\underline{\underline{x}})|_v < \Big(\prod_v |\det(L_{v1}, \dots, L_{vn})|_v\Big) \overline{|\underline{\underline{x}}|}^{-\delta}.$$

Then there are proper subspaces $S_1, \dots, \S_t$ of $\mathbb{Q}^n$, where

$$t = [8sd!)^{2^{26n} s^6 \delta^{-2}}]$$

such that all the solutions $\underline{\underline{x}} \in \mathbb{Z}^n$ lie in the union of $S_1, \dots, S_t$ and the box

$$\overline{|\underline{\underline{x}}|} \leqq \max_{\substack{1 \leqq i \leqq n \\ v \in S}} ((n!)^{8/\delta},\ H(L_{vi})).$$

In Theorems 1C and 1E, the reader should note that t, the bound on the number of subspaces, is independent of the linear forms.

The following theorem will turn out to be equivalent to Theorem 1D.

THEOREM 1D′. *Let K, S be as above. For $v \in S$, let L_{vi} $(i = 1, \dots, n)$ be n linearly independent linear forms over K. Then solutions $\underline{\underline{x}} \in \mathbb{P}^{n-1}(K)$ to the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} \left(\frac{|L_{vi}(\underline{\underline{x}})|_v}{\|\underline{\underline{x}}\|_v} \right)^{n_v} < \frac{1}{H_K(\underline{\underline{x}})^{n+\delta}} \tag{9.2}$$

where $\delta > 0$, lie in finitely many proper subspaces.

Remark. It is reasonable to consider $\underline{\underline{x}} \in \mathbb{P}^{n-1}(K)$, since both sides of the inequality are invariant under multiplying $\underline{\underline{x}}$ by a scalar.

LEMMA 1F. *Any element $\underline{\underline{x}}$ of $\mathbb{P}^{n-1}(K)$ has a set of coordinates $\underline{\underline{x}} = (x_1, \dots, x_n)$ such that*

(i) $|\underline{\underline{x}}|_v \leqq 1$ *for v non-Archimedean,*

(ii) $$\prod_{v \text{ non-Archimedean}} |\underline{\underline{x}}|_v^{n_v} \geqq 1/c_1(K),$$

(iii) $|\underline{\underline{x}}|_v \leqq c_2(K)|\underline{\underline{x}}|_w$ *for any Archimedean v, w.*

Remark. While (i) bounds $|\underline{\underline{x}}|_v$ from above for v non-Archimedean, (ii) says that $|\underline{\underline{x}}|_v$ can not be too small. Result (iii) says that all of the Archimedean absolute values are about the same.

Proof. Consider the ideal $\mathfrak{I}(\underline{\underline{x}})$ generated by $x_1, \dots, x_n$. There is some integral ideal $\mathfrak{A}$ in the same ideal class as $\mathfrak{I}(\underline{\underline{x}})$, and $\mathcal{N}(\mathfrak{A}) \leqq c_1(K)$. After multiplying $\underline{\underline{x}}$ by some

$\lambda \in K$, we get a new $\underline{\underline{x}}'$ with $\mathfrak{J}(\underline{\underline{x}}') = \mathfrak{A}$. After a change of notation, write $\mathfrak{J}(\underline{\underline{x}}) = \mathfrak{A}$. Then $x_1, \dots, x_n$ are integers in K, and so (i) holds.

If $(a) = \mathfrak{P}^{\nu}\mathfrak{P}_2^{\nu_2} \dots \mathfrak{P}_\ell^{\nu_\ell}$ and if $(p) = \mathfrak{P}^e \mathfrak{Q}_2^{e_2} \dots \mathfrak{Q}_k^{e_k}$, then the absolute value associated with $\mathfrak{P}$ has $|a|_{\mathfrak{P}} \; = p^{-\nu/e}$. Also if $\mathfrak{N}(\mathfrak{P}) = p^f$, then $n_{\mathfrak{P}} \; = ef$. (We are using rudimentary facts from algebraic number theory). Putting this together gives $|a|_{\mathfrak{P}}^{n_{\mathfrak{P}}} = \mathfrak{N}(\mathfrak{P})^{-\nu}$. So if

$$(x_i) = \prod_j \mathfrak{P}_j^{\nu_{ij}},$$

then

$$|\underline{\underline{x}}|_{\mathfrak{P}_j}^{n_{\mathfrak{P}_j}} = \mathfrak{N}(\mathfrak{P}_j)^{-\min(\nu_{1j},\dots,\nu_{nj})}.$$

On the other hand,

$$\mathfrak{J}(\underline{\underline{x}}) = \prod_j \mathfrak{P}_j^{\min(\nu_{1j},\dots,\nu_{nj})},$$

so we have

$$\prod_{v \text{ non-Archimedean}} |\underline{\underline{x}}|_v^{n_v} \quad = \prod_j \; |\underline{\underline{x}}|_{\mathfrak{P}_j}^{n_{\mathfrak{P}_j}} = \mathfrak{N}(\mathfrak{J}(\underline{\underline{x}}))^{-1},$$

and (ii) holds.

By Dirichlet's Unit Theorem, if $\alpha^{(1)}, \dots, \alpha^{(r_1)}$ correspond to real embeddings of K into $\mathbb{R}$ and $\alpha^{(r_1+1)}, \dots, \alpha^{(r_1+r_2)}, \overline{\alpha^{(r_1+1)}}, \dots, \overline{\alpha^{(r_1+r_2)}}$ correspond to the complex embeddings, then given any $C_1, \dots, C_{r_1+r_2}$, there exists a unit ϵ such that

$$|\epsilon^{(i)}| C_i \leqq |\epsilon^{(j)}| C_j \cdot c_2(K)$$

for $1 \leqq i, j \leqq r_1 + r_2$ and some constant $c_2(K)$. To prove (iii), we need

$$|\underline{\underline{x}}^{(i)}| \leqq c_2(K) |\underline{\underline{x}}^{(j)}|,$$

and this can be obtained by multiplying $\underline{\underline{x}}$ by a suitable unit ϵ.

We can now see that Theorem 1D implies Theorem 1D$'$. By the lemma, we have

$$\frac{1}{c_1(K)} \leqq \prod_{v \text{ non-Archimedean}} |\underline{\underline{x}}|_v^{n_v} \leqq 1,$$

more generally

$$\frac{1}{c_1(K)} \leqq \prod_{v \notin S} |\underline{\underline{x}}|_v^{n_v} \leqq 1.$$

In view of this inequality, (9.2) implies that

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{vi}(\underline{\underline{x}})|_v^{n_v} \leqq \frac{c_3(K)}{H_K(\underline{\underline{x}})^{\delta}}.$$

By the lemma again, we have

$$\frac{\overline{|\underline{\underline{x}}|}^{d}}{c_4(K)} \leqq H_K(\underline{\underline{x}}) \leqq \overline{|\underline{\underline{x}}|}^{d},$$

where

$$\overline{|\underline{\underline{x}}|} = \max_{\substack{1\leqq i\leqq n\\ 1\leqq j\leqq r_1+r_2}} |x_i^{(j)}| = \max_{v \text{ Archimedean}} |\underline{\underline{x}}|_v .$$

Then

$$\prod_{v\in S}\prod_{i=1}^{n} |L_{vi}(\underline{\underline{x}})|_v^{n_v} \leqq \frac{c_5(K,\delta)}{|\underline{\underline{x}}|^{d\delta}}$$

and Theorem 1D implies that the solutions lie in finitely many proper subspaces.

Exercise 1a. Show that Theorem 1D′ implies Theorem 1D.

§2. General S-unit Equations.

We now return to, and elaborate, on results stated at the beginning of Ch. IV, §3.

Let K be a number field and $S \subset M(K)$ a set of absolute values which contains all of the Archimedean ones. First, we consider equations of the form

$$x_0 + x_1 + \ldots + x_n = 0,$$

where $x_i \in U_S \quad (i = 0, \ldots, n)$. Evertse (1984), as well as Schlickewei and Van der Poorten (1982) have the following result.

THEOREM 2A. *An S-unit equation of the form*

$$x_0 + x_1 + \ldots + x_n = 0$$

has only finitely many solutions $\underline{\underline{x}} \in \mathbb{P}^n(U_S)$ for which no non-trivial subsum vanishes, i.e. for which

$$\sum_{i\in I} x_i \neq 0$$

when $\phi \neq I \neq \{0, 1, \ldots, n\}$.

Example. The equation $3^a \pm 3^b \pm 5^c \pm 5^d = 0$ is an S-unit equation if $S = \{\infty, 3, 5\}$. However, we get infinitely many solutions whose subsums vanish. So we see that the condition about no non-trivial subsum vanishing is a necessary hypothesis for this result.

Schlickewei had a slightly weaker version of this result before he obtained the general version above. Instead of requiring that no subsum vanish, he had imposed a condition about distinct primes in the summands.

COROLLARY 2B. *Given coefficients $\alpha_0, \dots, \alpha_n$ in $K^\times$, the equation*

$$\alpha_0 x_0 + \dots + \alpha_n x_n = 0$$

has at most finitely many solutions $\underline{\underline{x}} \in \mathbb{P}^n(U_S)$ for which no non-trivial subsum vanishes.

Proof. If S is suitably enlarged, we have $\alpha_i \in U_S$. Then set $x_i' = \alpha_i x_i$. By the theorem, there are only finitely many possibilities for $\underline{\underline{x}}'$ for which no subsum vanishes. (Notice that when S is enlarged, the theorem is strengthened since more S-units are allowed.)

Proof (of Theorem 2A). For $v \notin S$, we have $|x_i|_v = 1$, since $\underline{\underline{x}}$ is an S-unit. Then by the product formula, we have

$$\prod_{v \in S} |x_i|_v^{n_v} = 1 \qquad (i = 0, \dots, n),$$

and

$$\prod_{v \in S} \prod_{i=0}^{n} |x_i|_v^{n_v} = 1.$$

Now let $\underline{\underline{\tilde{x}}} = (x_0, \dots, x_{n-1})$. Then

$$\prod_{v \in S} \prod_{i=0}^{n} \left(\frac{|x_i|_v}{|\underline{\underline{\tilde{x}}}|_v} \right)^{n_v} = \frac{1}{H_K(\underline{\underline{\tilde{x}}})^{n+1}}.$$

For each $v \in S$, choose $i(v)$ in $0 \leqq i(v) \leqq n-1$ such that

$$|\underline{\underline{\tilde{x}}}|_v = |x_{i(v)}|_v,$$

and restrict to solutions where the $i(v)$ for $v \in S$ are fixed. There are $n^{\operatorname{card} S}$ such choices. Let the set of linear forms L_{vj} $(1 \leqq j \leqq n)$ be the set $\{X_0, X_1, \dots, X_{n-1}, (X_0 + \dots + X_{n-1})\} \backslash X_{i(v)}$. Then

$$\prod_{v \in S} \prod_{j=1}^{n} \left(\frac{|L_{vj}(\underline{\underline{x}})|_v}{|\underline{\underline{\tilde{x}}}|_v} \right)^{n_v} = \frac{1}{H_K(\underline{\underline{\tilde{x}}})^{n+1}},$$

and by the Subspace Theorem (version 1D′), the solutions $\underline{\underline{\tilde{x}}}$ lie in finitely many subspaces.

Say one such subspace is given by

$$c_0 x_0 + \dots + c_{n-1} x_{n-1} = 0.$$

Let $\mathfrak{J}_0$ be the set of i with $c_i \neq 0$. Then

$$\sum_{i \in \mathfrak{J}_0} c_i x_i = 0 \tag{2.1}$$

is an S-unit equation. Let $\mathfrak{J} \subset \mathfrak{J}_0$ with $\mathfrak{J} \neq \phi$ and consider solutions of

$$(2.2) \qquad \sum_{i \in \mathfrak{J}} c_i x_i = 0$$

for which no subsum vanishes. For every solution to (2.1), there is such a set $\mathfrak{J}$, and the number of such sets $\mathfrak{J}$ is finite. Apply the case $n' + 1 = |\mathfrak{J}|$ to the S-unit equation (2.2). (We are using induction as n). Up to proportionality, there are finitely many solutions. So it suffices to study solutions where $\{x_i\}_{i \in \mathfrak{J}}$ is proportional to a fixed $\{u_i\}_{i \in \mathfrak{J}}$, i.e. where

$$x_i = \xi u_i \qquad (i \in \mathfrak{J}).$$

Return to the given equation

$$\sum_{i=0}^{n} x_i = 0,$$

which we can rewrite as

$$\xi(\sum_{i \in \mathfrak{J}} u_i) + \sum_{i \notin \mathfrak{J}} x_i = 0.$$

If $\sum_{i \in \mathfrak{J}} u_i \neq 0$, this is an S-unit equation in $n + 1 - |\mathfrak{J}| + 1 = n + 2 - |\mathfrak{J}| \leqq n$ variables, namely ξ and x_i $(i \notin \mathfrak{J})$. By induction, we get finitely many solutions for which no subsum vanishes. On the other hand, if $\sum_{i \in \mathfrak{J}} u_i = 0$, then the subsum $\sum_{i \notin \mathfrak{J}} x_i$ vanishes as well and we are not interested in such solutions.

We have proved that there are only finitely many solutions to an S-unit equation for which no subsum vanishes. In the case where $K = \mathbb{Q}$, a bound has been given recently. Given coefficients $a_0, \ldots, a_n$ in $\mathbb{Q}^\times$, the number of solutions $\underline{\underline{x}} \in \mathbb{P}^n(U_S)$ of

$$a_0 x_0 + \ldots + a_n x_n = 0$$

for which no subsum vanishes is

$$\leqq (8s)^{2^{26n+4} s^6}.$$

This result is due to Schlickewei (to appear). Notice that the bound is independent of the coefficients $a_0, \ldots, a_n$. The case for general K is done in Schlickewei (to appear (d)).

§3. Norm Form Equations.

Let K be a number field with $[K : \mathbb{Q}] = d$ and $L(\underline{\underline{X}})$ be a linear form, say $L(\underline{\underline{X}}) = L(X_1, \ldots, X_n) = \alpha_1 X_1 + \ldots + \alpha_n X_n$ with $\alpha_i \in K$. Suppose that $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}$. Then $n \leqq d$ and L will not vanish on $\mathbb{Q}^n \backslash \underline{\underline{0}}$. As usual, denote the embeddings of K into $\mathbb{C}$ by $\alpha \mapsto \alpha^{(i)}$ $(i = 1, \ldots, d)$ and write $L^{(i)}(\underline{\underline{X}}) = \alpha_1^{(i)} X_1 + \ldots + \alpha_n^{(i)} X_n$. We write

$$\mathfrak{N}(L(\underline{\underline{X}})) = \prod_{i=1}^{d} L^{(i)}(\underline{\underline{X}}).$$

A *norm form* is any form F of the type $F(\underline{\underline{X}}) = a\mathfrak{N}(L(\underline{\underline{X}}))$ for some L as above and $a \in \mathbb{Q}^\times$. For a norm form F, we have $F(\underline{\underline{X}}) \in \mathbb{Q}[\underline{\underline{X}}]$, and F is trivially decomposable over the algebraic numbers as a product of linear factors.

By a *norm form equation* we mean an equation of the type

$$F(\underline{\underline{x}}) = m, \qquad \underline{\underline{x}} \in \mathbb{Z}^n,$$

where F is a norm form. When $d > n$ this is a generalization of the Thue equation. For if $n = 2$, the linear form $L(X, Y) = X - \alpha Y$ gives norm forms

$$F(X, Y) = a \prod_{i=1}^{d} (X - \alpha^{(i)} Y).$$

If $\deg \alpha = d \geqq 3$, then $F(x, y) = m$ is a Thue equation.

As $\underline{\underline{x}}$ runs through $\mathbb{Z}^n$, the linear expression $L(\underline{\underline{x}})$ will run through a set $\mathfrak{M} \subset K$. This set $\mathfrak{M}$ is a free $\mathbb{Z}$-module of rank n with basis $\alpha_1, \ldots, \alpha_n$. So we could rewrite the norm form equation as

$$a\mathfrak{N}(\mu) = m,$$

where $\mu \in \mathfrak{M}$.

Let $\mathbb{Q}\mathfrak{M}$ be the set of products $q\mu$ with $q \in \mathbb{Q}$, $\mu \in \mathfrak{M}$. Then $\mathbb{Q}\mathfrak{M}$ consists of $\alpha_1 x_1 + \ldots + \alpha_n x_n$ with $x_i \in \mathbb{Q} \quad (i = 1, \ldots, n)$. Let E be a subfield of K and let $\mathfrak{M}^E$ be the set of $\mu \in \mathfrak{M}$ such that

$$\lambda\mu \in \mathbb{Q}\mathfrak{M}$$

for every $\lambda \in E$. Then $\mathfrak{M}^E$ is a submodule of $\mathfrak{M}$. If $E \subset E'$, then $\mathfrak{M}^{E'} \subset \mathfrak{M}^E$; and we have $\mathfrak{M}^{\mathbb{Q}} = \mathfrak{M}$. The module $\mathfrak{M}$ is called *degenerate* if there is a field $E \subset K$ with $E \neq \mathbb{Q}$ and E not imaginary quadratic such that $\mathfrak{M}^E \neq \{0\}$. We say that F is *degenerate* if the corresponding $\mathfrak{M}$ is degenerate.

Example. Take $K = \mathbb{Q}(i, \sqrt{2})$, which has $d = 4$, and take $L(X, Y, Z) = X + iY + i\sqrt{2}Z$. Let $E = \mathbb{Q}(i)$. Then $\{x + iy : x, y \in \mathbb{Z}\} = \mathfrak{M}^E$. For if $x + iy + i\sqrt{2}z \in \mathfrak{M}^E$, then we would need $ix - y - \sqrt{2}z \in \mathbb{Q}\mathfrak{M}$, which forces $z = 0$. This does not show that $\mathfrak{M}$ is degenerate, though, since E is imaginary quadratic. We could also take $E = \mathbb{Q}(i\sqrt{2})$ to see $\mathfrak{M}^E = \{x + i\sqrt{2}z\} \neq \{0\}$, or take $E = \mathbb{Q}(\sqrt{2})$ to get $\mathfrak{M}^E = \{iy + i\sqrt{2}z\} \neq \{0\}$. So we see that $\mathfrak{M}$ is, in fact, degenerate.

Example. Suppose $d = p$ where p is a prime > 2, and $\mathfrak{M}$ is a $\mathbb{Z}$-module of rank n, where $n < p$. The only subfields of K are K and $\mathbb{Q}$, so we just need to consider $\mathfrak{M}^K$. Suppose $\mu \in K, \quad \mu \neq 0$. Notice that $\mathbb{Q}\mathfrak{M}$ is a vector space over $\mathbb{Q}$ of dimension n. As λ runs through K, then $\lambda\mu$ runs through K, a vector space of dimension d. So $K\mu = K \underset{\neq}{\supset} \mathbb{Q}\mathfrak{M}$ and thus $\mu \notin \mathfrak{M}^K$. Then $\mathfrak{M}^K = \{0\}$ and $\mathfrak{M}$ is not degenerate.

Example. If $n = d$, then $K = \mathbb{Q}\mathfrak{M}$ and $\mathfrak{M}^K = \mathfrak{M}$. If $K \neq \mathbb{Q}$ and K is not imaginary quadratic, then $\mathfrak{M}$ is degenerate.

Degeneracy is important, *for if F is non-degenerate, then the norm form equation $F(x, y) = m$ has only finitely many solutions.* (Schmidt (1972) and (1980) Lecture

Notes). On the other hand, if F is degenerate, there will exist some m so that $F(\underline{x}) = m$ has infinitely many solutions. Before justifying this last remark, we will consider the simplest case which has infinitely many solutions.

Example. Suppose $\alpha_1, \ldots, \alpha_d$ form an integral basis for K. Take $n = d$ and $L(\underline{\underline{X}}) = \alpha_1 X_1 + \ldots + \alpha_d X_d$. Consider the norm form equation $\mathfrak{N}(L(\underline{x})) = 1$. Then we seek solutions to the equation $\mathfrak{N}(\epsilon) = 1$ where $\epsilon = \alpha_1 x_1 + \ldots + \alpha_n x_n$. Thus ϵ is a unit. By Dirichlet's Theorem, we have infinitely many solutions unless K is $\mathbb{Q}$ or is imaginary quadratic.

In general, suppose that there exists a subfield E with $\mathfrak{M}^E \neq \{0\}$. We claim that if $\lambda \in E$, then not only is $\lambda\mathfrak{M}^E \subset \mathbb{Q}\mathfrak{M}$ but $\lambda\mathfrak{M}^E \subset \mathbb{Q}\mathfrak{M}^E$. For if $\mu \in \mathfrak{M}^E$, then $\lambda\mu \in \mathbb{Q}\mathfrak{M}$, so that $m\lambda\mu \in \mathfrak{M}$ for some positive integer m. Given $\lambda' \in E$, we have $\lambda' m\lambda\mu \in \mathbb{Q}\mathfrak{M}$, since $\lambda' m\lambda \in E$. This shows that $m\lambda\mu \in \mathfrak{M}^E$, thus $\lambda\mu \in \mathbb{Q}\mathfrak{M}^E$.

Now let $\mathfrak{O}^E_{\mathfrak{M}}$ be the set of $\lambda \in E$ with $\lambda\mathfrak{M}^E \subset \mathfrak{M}^E$. The set $\mathfrak{O}^E_{\mathfrak{M}}$ has the following properties:

(i) It is a ring containing 1.

(ii) It contains a field basis of E over $\mathbb{Q}$. For if $\lambda_1, \ldots, \lambda_e$ is a field basis, then $\lambda_i\mathfrak{M}^E \subset \frac{1}{m}\mathfrak{M}^E$ for some positive $m \in \mathbb{Z}$. Then $m\lambda_1, \ldots, m\lambda_e \in \mathfrak{O}^E_{\mathfrak{M}}$ form a field basis of E over $\mathbb{Q}$.

(iii) There exists an $\ell > 0$, $\ell \in \mathbb{Z}$ such that $\ell\mathfrak{O}^E_{\mathfrak{M}}$ contains only algebraic integers. For if $\mu \neq 0$ is in $\mathfrak{M}^E$ then $\lambda\mu \in \mathfrak{M}^E$ for every $\lambda \in \mathfrak{O}^E_{\mathfrak{M}}$. Then $\lambda \in \frac{1}{\mu}\mathfrak{M}^E$. But $\frac{1}{\mu}\mathfrak{M}^E$ is a free module with only finitely many generators, so there exists an ℓ so that $\frac{\ell}{\mu}\mathfrak{M}^E$ contains only algebraic integers. Then $\ell\mathfrak{O}^E_{\mathfrak{M}} \subset \frac{\ell}{\mu}\mathfrak{M}^E$ contains only algebraic integers.

Any subring of E which satisfies these three conditions is called an *order* of E. The set $\mathfrak{O}^E$ of all the integers in E is an example of an order. It is a fact that any order $\mathfrak{O}$ in E is contained in the *maximal order*, $\mathfrak{O}^E$. See Borevich and Shafarevich (1966) for a more complete discussion.

Example. Take $E = \mathbb{Q}(\sqrt{2})$. Then $\mathfrak{O}^E$ consists of $x + \sqrt{2}y$, with $x, y \in \mathbb{Z}$. Another example of an order consists of $x + 2\sqrt{2}\,y$ with $x,\ y \in \mathbb{Z}$.

We call $\mathfrak{O}^E_{\mathfrak{M}}$ the *ring of multipliers*. Take $\mathcal{E}^E_{\mathfrak{M}}$ to be the group of units of $\mathfrak{O}^E_{\mathfrak{M}}$ of norm $\mathfrak{N}_{E/\mathbb{Q}}(\epsilon) = 1$. By Dirichlet's Theorem on units, this group is infinite unless $E = \mathbb{Q}$ or E is imaginary quadratic. Now suppose that $\mu_0 \neq 0$ is in $\mathfrak{M}^E$. For $\epsilon \in \mathcal{E}^E_{\mathfrak{M}}$, we have $\mathfrak{N}(\epsilon\mu_0) = \mathfrak{N}(\mu_0)$ and $\epsilon\mu_0 \in \mathfrak{M}^E$. Then if $\mathfrak{N}(\mu_0) = m$, the norm-form equation

$$\mathfrak{N}(\mu) = m, \qquad \mu \in \mathfrak{M}^E$$

has infinitely many solutions.

So the condition of non-degeneracy is necessary to ensure the finiteness of the number of solutions.

Example. Let $K = \mathbb{Q}(i, \sqrt{2})$ and $F(x,y,z) = \mathfrak{N}(x + iy + i\sqrt{2}z)$. Then $\mathfrak{M}:\ x + iy + i\sqrt{2}z$. Now let $E = \mathbb{Q}(\sqrt{2})$. We have $\mathfrak{M}^E:\ iy + i\sqrt{2}z = i(y + \sqrt{2}z)$ and $\mathfrak{O}^E_{\mathfrak{M}} = \mathfrak{O}^E$, the ring of integers in E. We know that $\mathcal{E}^E_{\mathfrak{M}}$ is infinite and we have a unit $\epsilon = \sqrt{2} - 1$.

Any solution of $\mathfrak{N}_E(y + \sqrt{2}z) = \pm 1$ gives a solution $iy + i\sqrt{2}\,z \in \mathfrak{M}$ of $\mathfrak{N}(iy + i\sqrt{2}\,z) = 1$. Let us start with a particular solution of $\mathfrak{N}_E(y + \sqrt{2}\,z) = \mathfrak{N}_E(\mu) = \pm 1$, say with $\mu_0 = 1$ (so that $y_0 = 1,\ z_0 = 0$). By multiplication with powers of ϵ we obtain further solutions. Setting $\mu_t = \mu_0\epsilon^t = \epsilon^t$, we have $\mu_1 = \epsilon = \sqrt{2} - 1$ (so that $y_1 = -1,\ z_1 = 1$), $\mu_2 = (\sqrt{2}-1)^2 = 3 - 2\sqrt{2}$ (so that $y_2 = 3, z_2 = -2$), etc.

The reader may find a further discussion, especially about the degenerate case, in Schmidt (Lecture Notes, 1980). We return to the case where F is non-degenerate and consider bounds on the number of solutions.

THEOREM 3A. (Schmidt (1986b)). *If $F(\underline{X})$ is a non-degenerate norm form of degree d with coefficients in $\mathbb{Z}$, then the norm form equation*

$$F(\underline{x}) = m, \qquad \underline{x} \in \mathbb{Z}^n$$

has at most

$$d^{2^{30n}d^2}\ c_1(n,d,m)$$

solutions where $c_1(n,d,1) = 1$ and

$$c_1(n,d,m) = \binom{d}{n-1}^{\omega} d_{n-1}(m^d),$$

where ω is the number of distinct prime factors of m and $d_{n-1}(\ell)$ is the number of ways of writing $\ell = \ell_1 \dots \ell_{n-1}$ with $\ell_i > 0 \quad (i = 1, \dots, n-1)$.

As was seen in Section 6 of Chapter III, the general case follows from the case $m = 1$. Thus, one may concentrate on the norm-form equation

$$F(\underline{x}) = 1$$

and the bound

$$d^{2^{30n}d^2}. \tag{3.1}$$

In these Notes, we will not prove Theorem 3A and (3.1), but a variation. See Theorem 3B below.

Incidentally (Schmidt (1989b)) has also proved another bound in place of (3.1), namely

$$d^{(2n)^{n \cdot 2^{n+4}}}.$$

This second bound can probably be improved, removing one of the exponents by using some combinatorial techniques. The second bound is nicer for fixed n, since it grows only like a polynomial in terms of d.

How can this be generalized to the degenerate cases? There we would have finitely many solutions *up to multiplication by certain units.* An explicit bound so far has not been derived.

Also, what about asymptotic estimates for the number of solutions? The inequality $|F(\underline{x}| \leqq m$ defines some n-dimensional set of volume $c_F m^{n/d}$ where c_F depends on F only. Mahler (1934) has shown in the case $n = 2$, i.e. for the Thue case, that the number of solutions of this inequality is $\sim c_F m^{n/d}$ as $m \mapsto \infty$. Ramachandra (1969) proved this asymptotic formula for a class of norm form equations.

Now we will specialize the norm forms F somewhat. Let F be a norm form given by

$$F(\underline{\underline{X}}) = aL^{(1)}(\underline{\underline{X}}) \dots L^{(d)}(\underline{\underline{X}}),$$

and let E be a normal field containing the coefficients of $L^{(1)}, \dots, L^{(d)}$. Say that L has coefficients in a field K of degree d and $\mathbb{Q} \subset K \subset E$ where $E/\mathbb{Q}$ is normal. Let $G = \mathrm{Gal}(E/\mathbb{Q})$. Then G acts on the linear forms $\{L^{(1)}, \dots, L^{(d)}\}$ by acting on their coefficients. If $1 \leqq t \leqq d$ we say that G acts t *times transitively* if $L^{(1)}, \dots, L^{(d)}$ are distinct and if for any distinct integers $i_1, \dots, i_t$, there is a $\sigma \in G$ with

$$\sigma(L^{(j)}) = L^{(i_j)} \qquad (1 \leqq j \leqq t).$$

If, for instance, the Galois group of K is S_d, the symmetric group on d elements, then G is d times transitive.

THEOREM 3B. *Let everything be as above. If G acts $n-1$ times transitively and if any n among $L^{(1)}, \dots, L^{(d)}$ are linearly independent, then the number of solutions of $F(\underline{x}) = 1$ is*

$$\leqq d^{2^{30n}}.$$

It follows that forms as in Theorem 3B are non-degenerate. This could also be shown directly.

Example. Let $K = \mathbb{Q}(\alpha)$, where α is an algebraic integer of degree $d > 2$, and suppose $G = S_d$. Take

$$F(\underline{\underline{X}}) = \mathfrak{N}(X_1 + \alpha X_2 + \dots + \alpha^{d-2} X_{d-1}).$$

Then the hypotheses are satisfied

The class of equations treated in Theorem 3B includes Thue equations.

The remainder of this chapter will be devoted to the proof of Theorem 3B. (There are some extra technical difficulties for Theorem 3A.)

§4. A Reduction.

Given two norm forms F, G we say $F \sim G$ if $F = G^T$ for some $T \in SL(n, \mathbb{Z})$. Recall that $G^T(\underline{\underline{X}}) = G(T\underline{\underline{X}})$. The number of solutions of $F(\underline{x}) = 1$ is invariant under this equivalence relation. In Chapter III, Section 2, for a prime p, we exhibited certain transformations $T_0, T_1, \dots, T_p$ with $\det T_i = p$ such that

$$\mathbb{Z}^n = \bigcup_{i=0}^{p} T_i \mathbb{Z}^n.$$

So instead of studying $F(\underline{x}) = 1$, we could study the equations $F^{T_j}(\underline{x}) = 1 \quad (j = 0, 1, \dots, p)$. So what is the advantage of using F^{T_j}'s? From Chapter III, we know that $D(F^T) = (\det T)^{|I|}\, D(F)$, and then $D(F^T) \geqq p^{|I|}$. The advantage, then, is that we can consider forms whose semi-discriminant is large. The disadvantage is that we now have $p+1$ norm form equations to consider.

Let $N(n,d)$ be the maximum number of solutions to $F(\underline{x}) = 1$ for all norm forms F of degree d in n variables of the type described in Theorem 3B. Let $N(n,d,p)$ be the corresponding bound if we restrict to forms F with semi-discriminant $D(F) \geqq p^{|I|}$. Then

$$N(n,d) \leqq (p+1)N(n,d,p),$$

which is Lemma 2C of Chapter III. By Lemma 2B of the same chapter, we have

$$D(F) \leqq H^*(F)^{|I|n/d}.$$

Recall that I is the set of all n-tuples $i_1, \dots, i_n$ in $1 \leqq i_j \leqq d$ with $L^{(i_1)}, \dots, L^{(i_n)}$ linearly independent. (Under the hypothesis of Theorem 3B, I consists of all such n-types of distinct numbers.) Combining this last inequality with $D(F) \geqq p^{|I|}$, we see that we may restrict ourselves to forms with

$$H^*(F) \geqq p^{d/n}.$$

PROPOSITION 4A. *If $p > n^{10n^2}$, then*

$$N(n,d,p) < d^{2^{30n} - 10n^2}.$$

We may deduce the main theorem (3A) from this proposition. Recall that we need to show that the number of solutions to $F(\underline{x}) = 1$ is

$$\leqq d^{2^{30n}}.$$

We pick a prime p with

$$n^{10n^2} < p < 2n^{10n^2}.$$

Then we have

$$\begin{aligned} N(n,d) &\leqq (p+1)N(n,d,p) \\ &< d^{2^{30n}-10n^2} 2n^{10n^2} \\ &\leqq d^{2^{30n}} \end{aligned}$$

since $d > n$.

We may restrict still further. For a norm form $F = aL^{(1)} \dots L^{(d)}$, we have height $H^*(F) = H(L)^d \operatorname{cont} F$. In general, this height is not invariant under $\sim$. We let

$$\mathfrak{H}(F) = \min_{G \sim F} H^*(G).$$

This minimum exists, since among all forms L with coefficients in a given number field, there are only finitely many forms with $H(L) \leqq B$ for any bound B. Furthermore, this $\mathfrak{H}(F)$ is invariant under $\sim$.

So we restrict to norm forms F with $\mathfrak{H}(F) = H^*(F)$. We have seen that when $D(F) \geqq p^{|I|}$, we get $\mathfrak{H}(F) \geqq p^{d/n}$. In the proposition, $p > n^{10n^2}$, so the inequality becomes

$$(4.1) \qquad \mathfrak{H}(F) > n^{10dn}.$$

How does this apply to the linear form L? In counting solutions of $F(\underline{\underline{x}}) = 1$, we may suppose that $\operatorname{cont} F = 1$. Otherwise, we would have no solutions. Then (4.1) implies

$$H(L) > n^{10n}.$$

In the sections which follow, we will distinguish large and small solutions. *Small* solutions will be those with

$$|\underline{\underline{x}}| \leqq \mathfrak{H}(F)^{6nd^n} = H(L)^{6nd^{n+1}}.$$

The remaining solutions will be called *large* solutions.

§5. An Application of the Geometry of Numbers.

Let $L = \alpha_1 X_1 + \ldots + \alpha_n X_n$ with $\alpha_i \in K$, and write $L^{(i)} = \alpha_1^{(i)} X_1 + \ldots + \alpha_n^{(i)} X_n$, $(1 \leqq i \leqq d)$. Let

$$\underline{\underline{a}}_j = \begin{pmatrix} \alpha_j^{(1)} \\ \vdots \\ \alpha_j^{(d)} \end{pmatrix}, \qquad (1 \leqq j \leqq n)$$

and $\underline{\underline{A}} = \underline{\underline{a}}_1 \wedge \ldots \wedge \underline{\underline{a}}_n$. Then $\underline{\underline{A}}$ lies in $\mathbb{C}^\ell$, where $\ell = \binom{n}{d}$. If $\underline{\underline{A}} = (\beta_1, \ldots, \beta_\ell)$, introduce

$$\Delta(L) = |\underline{\underline{A}}| = \sqrt{|\beta_1|^2 + \ldots + |\beta_\ell|^2}.$$

Then it is easily seen that

$$\Delta(L^T) = \Delta(L)$$

for $T \in SL(n, \mathbb{Z})$.

LEMMA 5A. *Given the notation above,*

$$|a|^{n/d} \Delta(L) \geqq \frac{V(n)}{2^n n^{3/2}} d^{n/2} (\operatorname{cont} F)^{(n-1)/d} \mathfrak{H}(F)^{1/d},$$

where $V(n)$ is the volume of the unit ball in $\mathbb{R}^n$.

Notice that both sides are invariant under $\sim$. The right-hand side depends only on F, but the left-hand side depends on how we write $F = aL^{(1)} \ldots L^{(d)}$. We could write instead $F = a'L'^{(1)} \ldots L'^{(d)}$, where $L' = \lambda L$. Then $a' = a/\mathfrak{N}(\lambda)$, but there is no simple way to express $\Delta(L')$ in terms of λ and $\Delta(L)$.

The matrix

$$\left(\alpha_j^{(i)}\right) \qquad (1 \leqq i \leqq d,\ 1 \leqq j \leqq n)$$

has rank n, so $\underline{\underline{a}}_1, \dots, \underline{\underline{a}}_n$ are linearly independent. Let Λ be the set of all linear combinations

$$x_1 \underline{\underline{a}}_1 + \dots + x_n \underline{\underline{a}}_n,$$

where $x_i \in \mathbb{Z}$. We will see that Λ may be interpreted as an n-dimensional lattice in some Euclidean space.

Suppose that the field K has r_1 real embeddings and r_2 pairs of complex conjugate embeddings. Then $r_1 + 2r_2 = d$. Suppose

$$\alpha \longmapsto \alpha^{(i)}$$

is real for $1 \leqq i \leqq r_1$, and

$$\alpha \longmapsto \alpha^{(i)}, \quad \alpha \longmapsto \alpha^{(i+r_2)}$$

are complex conjugate embeddings for $r_1 + 1 \leqq i \leqq r_1 + r_2$. Let E^d be the space of vectors

$$\begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix}$$

where $z_1, \dots, z_{r_1}$ are real and z_i, z_{i+r_2} are complex conjugates for $r_1 + 1 \leqq i \leqq r_1 + r_2$. Then E^d is a vector space over $\mathbb{R}$ of dimension d. Introduce an inner product

$$\underline{\underline{z}} \cdot \underline{\underline{z}}' = z_1 \overline{z}_1' + \dots + z_d \overline{z}_d'$$

and a norm

$$|\underline{\underline{z}}| = \sqrt{\underline{\underline{z}} \cdot \underline{\underline{z}}}$$

on E^d.

Exercise 5a. Show that, with this inner product, E^d is a Euclidean vector space.

By inspection, $\underline{\underline{a}}_i \in E^d$. Then we may interpret Λ as an n-dimensional lattice in E^d, as mentioned earlier. Now we may consider successive minima. In other words, introduce $\mu_1, \dots, \mu_n$ where μ_j is the least positive real number such that there are j linearly independent points of Λ with $|\underline{\underline{g}}| \leqq \mu_j$. Here $|\quad|$ is the norm above.

If $\underline{\underline{z}} = u_1\, \underline{\underline{a}}_1 + \dots + u_n\, \underline{\underline{a}}_n \in \Lambda$, with components $z^{(i)}$, then $z^{(i)} = L^{(i)}(u_1, \dots, u_n)$. We have

$$|a|\ |z^{(1)} \dots z^{(d)}| = |F(u_1, \dots, u_n)| \geqq \operatorname{cont} F,$$

unless $u_1 = \dots = u_n = 0$. So every non-zero lattice point $\underline{\underline{z}}$ has

$$|z^{(1)} \dots z^{(d)}| \geqq (\operatorname{cont} F)/|a|.$$

The Arithmetic-Geometric Inequality gives

$$\begin{aligned} |\underline{\underline{z}}| &= \sqrt{|z^{(1)}|^2 + \dots + |z^{(d)}|^2} \\ &\geqq \sqrt{d \sqrt[d]{|z^{(1)}|^2 \dots |z^{(d)}|^2}} \\ &\geqq \sqrt{d}\sqrt[d]{(\operatorname{cont} F)/|a|}. \end{aligned}$$

We may conclude that

$$\mu_1 \geqq \sqrt{d}\ \sqrt[d]{(\operatorname{cont} F)/|a|}. \tag{5.1}$$

Now suppose that $\underline{\underline{b}}_1, \dots, \underline{\underline{b}}_n$ is another basis of Λ. Say

$$\underline{\underline{b}}_j = \begin{pmatrix} \beta_j^{(1)} \\ \vdots \\ \beta_j^{(d)} \end{pmatrix} = m_{j1}\ \underline{\underline{a}}_1 + \dots + m_{jn}\ \underline{\underline{a}}_n,$$

where the matrix (m_{jk}) is in $SL(n, \mathbb{Z})$. Introduce the row vectors

$$\underline{\underline{\alpha}}^{(i)} = (\alpha_1^{(i)}, \dots, \alpha_n^{(i)})$$

and

$$\underline{\underline{\beta}}^{(i)} = (\beta_1^{(i)}, \dots, \beta_n^{(i)}).$$

Then we have

$$\begin{aligned} \beta_j^{(i)} &= m_{j1}\ \alpha_1^{(i)} + \dots + m_{jn}\ \alpha_n^{(i)} \\ &= \alpha_1^{(i)} m_{j1} + \dots + \alpha_n^{(i)}\ m_{jn}, \end{aligned}$$

so $\underline{\underline{\beta}}^{(i)} = \underline{\underline{\alpha}}^{(i)} M^t$, where M^t is the transpose of M. Let

$$\begin{aligned} F^{M^t}(\underline{\underline{X}}) &= F(M^t \underline{\underline{X}}) \\ &= a \prod_{i=1}^{d} (\underline{\underline{\alpha}}^{(i)} M^t \underline{\underline{X}}) \\ &= a \prod_{i=1}^{d} (\underline{\underline{\beta}}^{(i)} \underline{\underline{X}}). \end{aligned}$$

Since $F^{M^t} \sim F$, we have

$$H^*(F^{M^t}) \geqq \mathfrak{H}(F),$$

so that

$$|a|^2 \prod_{i=1}^{d} |\underline{\underline{\beta}}^{(i)}|^2 \geqq \mathfrak{H}(F)^2.$$

Using the Arithmetic-Geometric Inequality, we get

$$\sum_{i=1}^{d} |\underline{\underline{\beta}}^{(i)}|^2 \geqq d(\mathfrak{H}(F)/|a|)^{2/d}.$$

Recall that

$$\underline{\underline{\beta}}^{(i)} = (\beta_1^{(i)}, \dots, \beta_n^{(i)}) \quad \text{and} \quad \underline{\underline{b}}_j = \begin{pmatrix} \beta_j^{(i)} \\ \vdots \\ \beta_j^{(d)} \end{pmatrix}.$$

Therefore

$$\sum_{j=1}^{n} |\underline{\underline{b}}_j|^2 \geqq d(\mathfrak{H}(F)/|a|)^{2/d}, \tag{5.2}$$

which says that a basis $\underline{\underline{b}}_1, \ldots, \underline{\underline{b}}_n$ can not be too small.

Given our lattice Λ and any basis $\underline{\underline{b}}_1, \ldots, \underline{\underline{b}}_n$ of Λ, there are linearly independent lattice points $\underline{\underline{g}}_1, \ldots, \underline{\underline{g}}_n$ such that

$$|\underline{\underline{g}}_1| = \mu_1, \ |\underline{\underline{g_2}}| = \mu_2, \ldots, |\underline{\underline{g}}_n| = \mu_n,$$

where $\mu_1, \ldots, \mu_n$ are the successive minima. For $n = 2$ these $\underline{\underline{g}}_i$ necessarily form a basis, but for $n > 2$, they are not necessarily a basis. However, one can show that there is a basis $\underline{\underline{b}}_1, \ldots, \underline{\underline{b}}_n$ with the property that

$$|\underline{\underline{b}}_j| \leqq j\mu_j \qquad (j = 1, \ldots, n).$$

Exercise 5b. Verify this last statement. The reader may consult Cassels' text on the Geometry of Numbers (1959).

Given such a basis, we have

$$\sum_{j=1}^{n} |\underline{\underline{b}}_j|^2 \leqq \left(\sum_{j=1}^{n} j^2 \right) \mu_n^2 \leqq n^3 \mu_n^2.$$

If we combine this with (5.2) we obtain

$$\mu_n \geqq \frac{d^{1/2}}{n^{3/2}} \, (\mathfrak{H}(F)/|a|)^{1/d}.$$

From (5.1), we also had

$$\mu_j \geqq d^{1/2} \, (\operatorname{cont} F/|a|)^{1/d} \qquad (j = 1, \ldots, n-1).$$

Taking the product of these inequalities we see that

$$\mu_1 \mu_2 \ldots \mu_n \geqq \frac{d^{n/2}}{n^{3/2} \, |a|^{n/d}} \, (\operatorname{cont} F)^{(n-1)/d} \, \mathfrak{H}(F)^{1/d}.$$

By Minkowski's Second Theorem (2E of Chapter I), we have

$$\mu_1 \ldots \mu_n V(n) \leqq 2^n \, \det \Lambda,$$

so that

$$\det \Lambda \geqq \frac{V(n)}{2^n \, n^{3/2} \, |a|^{n/d}} \, d^{n/2} \, (\operatorname{cont} F)^{(n-1)/d} \, \mathfrak{H}(F)^{1/d}.$$

But

$$\det \Lambda = |\det \underline{\underline{a}}_i \, \overline{\underline{\underline{a}}}_j|^{1/2}$$
$$= |\underline{\underline{a}}_1 \wedge \ldots \wedge \underline{\underline{a}}_n| = \Delta(L),$$

and the proof is complete.

§6. Products of Linear Forms.

LEMMA 6A. *Suppose $F(\underline{\underline{X}}) = aL^{(1)}(\underline{\underline{X}}) \ldots L^{(d)}(\underline{\underline{X}})$ is a norm form with coefficients in $\mathbb{Z}$. Suppose $\underline{\underline{x}} \in \mathbb{Z}^n$ is a solution of*

$$F(\underline{\underline{x}}) = 1.$$

Then there exist $i_1, \ldots, i_n$ with $1 \leqq i_1 < \ldots < i_n \leqq d$ such that

$$|L^{(i_1)}(\underline{\underline{x}}) \ldots L^{(i_n)}(\underline{\underline{x}})| \leqq \frac{2^n n^{3/2}}{(n!)^{1/2} V(n)} \, |\det(L^{(i_1)}, \ldots, L^{(i_n)})\, |\mathfrak{H}(F)^{-1/d}.$$

The significant term on the right hand side is $\mathfrak{H}(F)^{-1/d}$. Why would such a lemma be useful? Recall, in the case of the Thue equation, if $a|x - \alpha_1 y| \ldots |x - \alpha_n y| = 1$, then $|\alpha_i y - x|$ was small for some i. Then $|\alpha_i y - x| \; |\alpha_j y - x|$ was small for any j. We now have an analogue. Here we have n variables, and we can find some n of the linear forms such that their product is small at $\underline{\underline{x}}$.

Proof. We have

$$aL^{(1)}(\underline{\underline{x}}) \ldots L^{(d)}(\underline{\underline{x}}) = 1.$$

Introduce

$$V(\underline{\underline{X}}) = L(\underline{\underline{X}})/L(\underline{\underline{x}}),$$

so that

$$F(\underline{\underline{X}}) = V^{(1)}(\underline{\underline{X}}) \ldots V^{(d)}(\underline{\underline{X}}).$$

Now apply the lemma of Section 5 with $a = 1$, $\operatorname{cont} F = 1$, and V in place of L. We have $\operatorname{cont} F = 1$ because we have an integer solution to $F(\underline{\underline{x}}) = 1$. The lemma gives

$$\Delta(V) \geqq \frac{V(n)}{2^n n^{3/2}} \, d^{n/2} \, \mathfrak{H}(F)^{1/d}.$$

Let

$$\underline{\underline{a}}_j = \begin{pmatrix} \alpha_j^{(1)}/L^{(1)}(\underline{\underline{x}}) \\ \vdots \\ \alpha_j^{(d)}/L^{(d)}(\underline{\underline{x}}) \end{pmatrix}.$$

Then

$$\Delta(V)^2 = |\underline{\underline{a}}_1 \wedge \ldots \wedge \underline{\underline{a}}_n|^2 = |\underline{\underline{A}}|^2 \geqq \frac{V(n)^2}{4^n n^3} \, d^n \, \mathfrak{H}(F)^{2/d}.$$

Now let $D(i_1,\dots i_n)$ be the determinant of the submatrix of $(\alpha_j^{(i)}/L^{(i)}(\underline{\underline{x}}))$ where i is among $i_1,\dots,i_n$. Then

$$|A|^2 = \sum_{1\leqq i_1<\dots<i_n\leq d} |D(i_1,\dots,i_n)|^2,$$

and the number of n-tuples in the sum is $\binom{d}{n} \leqq \frac{d^n}{n!}$. Then some $D(i_1,\dots,i_n)$ satisfies

$$|D(i_1,\dots,i_n)|^2 \geqq \frac{V(n)^2\, n!}{4^n\, n^3}\,\mathfrak{H}(F)^{2/d},$$

and

$$|D(i_1,\dots,i_n)| \geqq \frac{V(n)(n!)^{1/2}}{2^n\, n^{3/2}}\,\mathfrak{H}(F)^{1/d}.$$

But

$$|D(i_1,\dots,i_n)| = \frac{|\det(L^{(i_1)},\dots,L^{(i_n)})|}{|L^{(i_1)}(\underline{\underline{x}})\dots L^{(i_n)}(\underline{\underline{x}})|},$$

so we can get an upper bound for $|L^{(i_1)}(\underline{\underline{x}})\dots L^{(i_n)}(\underline{\underline{x}})|$ in terms of $|\det(L^{(i_1)},\dots,L^{(i_n)})|$. We have

$$|L^{(i_1)}(\underline{\underline{x}})\dots L^{(i_n)}(\underline{\underline{x}})| \leqq \frac{|\det(L^{(i_1)},\dots,L^{(i_n)})|}{P},$$

where

$$P = \frac{\mathfrak{H}(F)^{1/d}\,(n!)^{1/2}\,V(n)}{2^n\, n^{3/2}}.$$

In the case of the Thue equation, we used a Gap Principle to get a bound on the number of solutions. We will do a similar thing in the next section.

§7. A Generalized Gap Principle.

We first present a simple argument in diophantine approximations. Consider rational approximations $\frac{x}{y}$ to a real number α with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{Py^2},$$

and say $P \geqq 4$. Given such reduced and distinct $x_1/y_1,\dots,x_\nu/y_\nu$ with $y_1 \leqq \dots \leqq y_\nu$, then

$$\frac{1}{y_{j-1}y_j} \leqq \left|\alpha - \frac{x_{j-1}}{y_{j-1}}\right| + \left|\alpha - \frac{x_j}{y_j}\right| < \frac{2}{P\,y_{j-1}^2},$$

therefore

$$y_j > \frac{P}{2}\, y_{j-1},$$

and so

$$y_\nu \geqq (P/2)^{\nu-1}.$$

The number of such approximations in reduced form with $1 \leqq y \leqq B$ is

$$\leqq 1 + \frac{\log B}{\log(P/2)} \leqq 1 + 2\,\frac{\log B}{\log P}\,.$$

We now want to generalize this.

LEMMA 7A. *Suppose $L_1, \dots, L_n$ are $n > 1$ linearly independent linear forms in n variables with complex coefficients. Suppose*

$$(n!)^4 \leqq P \leqq B$$

and put

$$Q = (\log B)/\log P.$$

Then the integer points $\underline{\underline{x}}$ in the ball $|\underline{\underline{x}}| \leqq B$ with

$$|L_1(\underline{\underline{x}}) \dots L_n(\underline{\underline{x}})| \leqq |\det(L_1, \dots, L_n)| P^{-1}$$

lie in the union of at most

$$n^{3n} Q^{n-1}$$

proper subspaces of $\mathbb{Q}^n$.

Proof. The proof falls into two parts, the first being a reduction of the problem.

(A) If $L(\underline{\underline{X}}) = \alpha_1 X_1 + \dots + \alpha_n X_n = \underline{\underline{\alpha}}\,\underline{\underline{X}}$ and $M = \underline{\underline{\beta}}\,\underline{\underline{X}}$, then let $(L, M) = \underline{\underline{\alpha\overline{\beta}}}$ and $|L| = \sqrt{(L, L)}$. We will reduce to the case where $L_1, \dots, L_n$ are pairwise orthogonal, i.e. $(L_i, L_j) = 0$ for $i \neq j$.

If $L_i(\underline{\underline{X}}) = \underline{\underline{\alpha}}_i\,\underline{\underline{X}}$, then let

$$\hat{\underline{\underline{\alpha}}}_i = (-1)^{i-1}\, \overline{\underline{\underline{\alpha}}_1 \wedge \dots \wedge \underline{\underline{\alpha}}_{i-1} \wedge \underline{\underline{\alpha}}_{i+1} \wedge \dots \wedge \underline{\underline{\alpha}}_n},$$

which has n components since $\binom{n}{n-1} = n$. We have

$$\underline{\underline{\alpha}}_i\,\bar{\hat{\underline{\underline{\alpha}}}}_j = \delta_{ij} \det(\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_n), \tag{7.1}$$

where δ_{ij} is the Kronecker symbol. This last statement is true because the coordinates of the $\bar{\hat{\underline{\underline{\alpha}}}}_j$ are the minors of the matrix with rows $\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_n$, so we get the determinant expanded about the ith row.

The assertion of the lemma is invariant under replacing L_i by the multiple $\lambda_i L_i$. We choose

$$\lambda_i = |\hat{\underline{\underline{\alpha}}}_i| / (|\hat{\underline{\underline{\alpha}}}_1| \cdots |\hat{\underline{\underline{\alpha}}}_n|)^{1/(n-1)}$$

and replace

$$\underline{\underline{\alpha}}_i \mapsto \lambda_i \underline{\underline{\alpha}}_i,$$

so that

$$\hat{\underline{\underline{\alpha}}}_i \mapsto \hat{\underline{\underline{\alpha}}}_i / |\hat{\underline{\underline{\alpha}}}_i|.$$

After such a transformation, we may suppose that $|\underline{\underline{\hat{\alpha}}}_1| = \ldots = |\underline{\underline{\hat{\alpha}}}_n| = 1$.

Suppose that we restrict our attention to solutions where

$$|L_n(\underline{\underline{x}})| = \max_{1\leqq i\leqq n} |L_i(\underline{\underline{x}})|.$$

It suffices to show that the number of subspaces required under this restriction is

$$\leqq \frac{1}{n} n^{3n} Q^{n-1}.$$

Write

$$\underline{\underline{\hat{\alpha}}}_n = c_1 \underline{\underline{\alpha}}_1 + \ldots + c_n \underline{\underline{\alpha}}_n.$$

We have

$$\begin{aligned} \underline{\underline{\hat{\alpha}}}_n \, \underline{\underline{\bar{\hat{\alpha}}}}_j &= \sum_{i=1}^{n} c_i \, \underline{\underline{\alpha}}_i \underline{\underline{\bar{\hat{\alpha}}}}_j \\ &= c_j \det(\underline{\underline{\alpha}}_1, \ldots, \underline{\underline{\alpha}}_n) \end{aligned}$$

by (7.1). Looking at the left-hand side, we know that

$$|\underline{\underline{\hat{\alpha}}}_n \, \underline{\underline{\bar{\hat{\alpha}}}}_j| \leqq 1$$

with equality when $j = n$. Thus

$$|c_j| \leqq |c_n| \qquad\qquad (j = 1, \ldots, n).$$

Put

$$\begin{aligned} \underline{\underline{\alpha}}'_n &= \underline{\underline{\hat{\alpha}}}_n / c_n \\ &= c'_1 \underline{\underline{\alpha}}_1 + \ldots + c'_{n-1} \underline{\underline{\alpha}}_{n-1} + \underline{\underline{\alpha}}_n \end{aligned}$$

with $|c'_i| \leqq 1$, and put

$$L'_n(\underline{\underline{X}}) = \underline{\underline{\alpha}}'_n \underline{\underline{X}}.$$

We have

$$\det(L_1, \ldots, L_{n-1}, L_n) = \det(L_1, \ldots, L_{n-1}, L'_n)$$

and L'_n is orthogonal to $L_1, \ldots, L_{n-1}$. Also

$$L'_n(\underline{\underline{x}}) = c'_1 L_1(\underline{\underline{x}}) + \ldots + c'_{n-1} L_{n-1}(\underline{\underline{x}}) + L_n(\underline{\underline{x}}),$$

so that

$$|L'_n(\underline{\underline{x}})| \leqq n |L_n(\underline{\underline{x}})|,$$

since $|c'_i| \leqq 1$ and $|L_n(\underline{\underline{x}})| = \max_{1\leqq i \leqq n} |L_i(\underline{\underline{x}})|$. Then

$$\begin{aligned} |L_1(\underline{\underline{x}}) \ldots L_{n-1}(\underline{\underline{x}}) L'_n(\underline{\underline{x}})| &\leqq n |L_1(\underline{\underline{x}}) \ldots L_n(\underline{\underline{x}})| \\ &\leqq n |\det(L_1, \ldots, L_n)| P^{-1} \\ &= n |\det(L_1, \ldots, L'_n)| P^{-1}. \end{aligned}$$

Thus it suffices to show that when L_n is orthogonal to $L_1, \ldots, L_{n-1}$, then the solutions of

$$|\underline{x}| \leqq B$$

and

$$|L_1(\underline{x}) \ldots L_n(\underline{x})| \leqq n|\det(L_1, \ldots, L_n)|P^{-1}$$

lie in the union of not more than

$$\frac{1}{n} n^{3n} Q^{n-1}$$

proper subspaces. This is the key reduction.

We repeat this argument. As before, we may suppose that $|\underline{\hat{\alpha}}_1| = \ldots |\underline{\hat{\alpha}}_n| = 1$ and we restrict to solutions with

$$|L_{n-1}(\underline{x})| = \max_{1 \leqq i \leqq n-1} |L_i(\underline{x})|.$$

Again, write

$$\underline{\hat{\alpha}}_{n-1} = c_1 \underline{\alpha}_1 + \ldots + c_{n-1} \underline{\alpha}_{n-1},$$

where $\underline{\alpha}_n$ does not appear since $\underline{\hat{\alpha}}_{n-1}$ is orthogonal to $\underline{\alpha}_n$ and the orthogonal complement of $\underline{\alpha}_n$ is spanned by $\underline{\alpha}_1, \ldots, \underline{\alpha}_{n-1}$. We have $|c_j| \leqq |c_{n-1}| \quad (1 \leqq j \leqq n-1)$, and we take

$$\underline{\alpha}'_{n-1} = \underline{\hat{\alpha}}_{n-1}/c_{n-1}$$

and

$$L'_{n-1}(\underline{X}) = \underline{\alpha}'_{n-1} \underline{X}.$$

Then

$$|L'_{n-1}(\underline{x})| \leqq (n-1)|L_{n-1}(\underline{x})|.$$

Thus it suffices to show that when L_n is orthogonal to $L_i \quad (i \neq n)$ and L_{n-1} is orthogonal to $L_i \quad (i \neq n-1)$, then the solutions of

$$|\underline{x}| \leqq B$$

and

$$|L_1(\underline{x}) \ldots L_n(\underline{x})| < n(n-1)|\det(L_1, \ldots, L_n)|P^{-1}$$

lie in no more than

$$\frac{1}{n(n-1)} n^{3n} Q^{n-1}$$

proper subspaces.

Applying this argument repeatedly, we get the following reduction. *If $L_1, \ldots, L_n$ are pairwise orthogonal, then the solutions of*

$$|\underline{x}| \leqq B$$

and

$$|L_n(\underline{x})\dots L_n(\underline{x})| < n!\,|\det(L_1,\dots,L_n)|P^{-1}$$

lie in at most

$$(2n^2)^{n-1}\,Q^{n-1} \leqq \frac{1}{n!}\,n^{3n}Q^{n-1}$$

proper subspaces.

We may reduce even further by supposing that $(L_i, L_j) = \delta_{ij}$. To do so, just multiply by suitable factors to make $|L_i| = 1$ for $1 \leqq i \leqq n$. Then $|\det(L_1,\dots,L_n)| = 1$.

(B) Having completed the reduction process, we study solutions $\underline{x}$ to

$$|L_1(\underline{x})\dots L_n(\underline{x})| < n!\,P^{-1},$$
$$|\underline{x}| \leqq B$$

and therefore

$$|L_i(\underline{x})| \leqq B \qquad\qquad (i = 1,\dots,n).$$

Put

$$C = (P/(n!)^2)^{1/(n-1)},$$

so that

$$|L_1(\underline{x})\dots L_n(\underline{x})| < 1/(n!\;C^{n-1}),$$

and put

$$R = \log(n!B^n)/\log C.$$

We subdivide the solutions into several classes. Either for some i in $1 \leqq i \leqq n-1$ we have

$$|L_i(\underline{x})| < B\,C^{-R} = B^{1-n}/n!, \qquad\quad (E_i)$$

or we have

$$B\,C^{-p_i-1} \leqq |L_i(\underline{x})| \leqq B\,C^{-p_i} \qquad (i = 1,\dots,n-1) \qquad (E_{p_1,\dots,p_{n-1}}),$$

for integers $p_1,\dots,p_{n-1}$ with $0 \leqq p_i \leqq R$. If $\underline{x}$ is a solution in one of the first classes, say E_i, then one of the first $n-1$ forms, namely $L_i(\underline{x})$, is really small at $\underline{x}$. The second set of classes covers the cases where this is not true.

Let $\underline{x}_1,\dots,\underline{x}_n$ be solutions in some class E_i. Then

$$\begin{aligned}|\det(\underline{x}_1,\dots,\underline{x}_n)| &= |\det(L_1,\dots,L_n)| \quad |\det(\underline{x}_1,\dots,\underline{x}_n)|\\ &= |\det_{1\leqq k,\; j\leqq n} L_k(\underline{x}_j)|\\ &< n!\,B^{n-1}\cdot\frac{1}{n!}\;B^{1-n} = 1.\end{aligned}$$

Then $\det(\underline{x}_1,\dots,\underline{x}_n) = 0$ and any n solutions in this class are linearly dependent. In other words, all of the solutions in a given E_i must lie in a single subspace. So counting solutions in $E_1,\dots,E_{n-1}$, we have at most $n-1$ subspaces.

Now consider solutions in one of the second classes. We have

$$|L_1(\underline{\underline{x}}) \dots L_n(\underline{\underline{x}})| < 1/(n!\,C^{n-1}),$$

so

$$|L_n(\underline{\underline{x}})| < \frac{C^{p_1+\dots+p_{n-1}}}{n!\;B^{n-1}}\,.$$

Let $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_n$ be solutions in this class, called $E_{p_1,\dots,p_{n-1}}$. Then

$$\begin{aligned}
|\det(\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_n) = | &\det_{1 \leqq k,\ j \leqq n} \; L_k(\underline{\underline{x}}_j)| \\
&< n!\,B^{n-1}\,C^{-p_1-\dots-p_{n-1}}\;\frac{C^{p_1+\dots+p_{n-1}}}{n!\,B^{n-1}} \\
&= 1,
\end{aligned}$$

and $\underline{\underline{x}}_1, \dots, \underline{\underline{x}}_n$ are linearly dependent, as before. In this case, how many subspaces may we have? In other words, how many classes can occur? We have $p_1, \dots, p_{n-1}$ with $0 \leqq p_i \leqq R$, which gives no more than

$$(R+1)^{n-1}$$

possibilities. Recall that

$$R = \frac{\log(n!\,B^n)}{\log C}\,,$$

and by hypothesis

$$n!\,B^n < B^{n+1}\,.$$

We also have

$$C = \left(\frac{P}{(n!)^2}\right)^{1/(n-1)} \geqq P^{1/(2n-2)},$$

by hypothesis. Combining these gives

$$R < \frac{\log B^{n+1}}{\log P^{1/(2n-2)}} = (2n^2-2)Q,$$

and we have

$$(R+1)^{n-1} \leqq ((2n^2-2)Q+1)^{n-1}$$

subspaces.

All together, the total number of subspaces is

$$\begin{aligned}
&\leqq n-1+((2n^2-1)Q)^{n-1} \\
&\leqq (2n^2 Q)^{n-1},
\end{aligned}$$

which is what we asserted.

§8. Small Solutions.

In Section 6, we saw that $|F(\underline{x})| = 1$ implies that for some $i_1 < \ldots < i_n$, we have

$$|L^{(i_1)}(\underline{x}) \ldots L^{(i_n)}(\underline{x})| < |\det(L^{(i_1)}, \ldots, L^{(i_n)})| P^{-1}, \tag{8.1}$$

where

$$P = \frac{V(n)(n!)^{1/2}}{2^n\, n^{3/2}}\, \mathfrak{H}(F)^{1/d}.$$

Exercise 8a. Show that

$$(n!)^{1/2}\, V(n) > 1/(2\pi)^{n/2}.$$

Using this exercise, we get

$$P > \frac{1}{(2\sqrt{2\pi})^n\, n^{3/2}}\, \mathfrak{H}(F)^{1/d} > \mathfrak{H}(F)^{1/2d} > (n!)^4,$$

where the last two inequalities follow since $\mathfrak{H}(F) > n^{10nd}$ by (4.1).

As we mentioned previously, small solutions will be those with

$$|\underline{x}| \leqq \mathfrak{H}(F)^{6nd^n}.$$

Let this bound be B. By Lemma 7A, the small solutions satisfying (8.1) lie in no more than

$$n^{3n}\, (\log B / \log P)^{n-1}$$

subspaces, and we have

$$\begin{aligned} n^{3n}(\log B / \log P)^{n-1} &\leqq n^{3n} \left(\frac{6nd^n \log \mathfrak{H}(F)}{(\log \mathfrak{H}(F))/2d} \right)^{n-1} \\ &\leqq 12^n\, n^{4n}\, d^{n^2-1}\ . \end{aligned}$$

Counting the number of possibilities for the n-tuple $1 \leqq i_1 < \ldots < i_n \leqq d$, which is $\binom{d}{n} \leqq d^n$, we get the following result.

PROPOSITION 8A. *Under our hypotheses, the small solutions of*

$$|F(\underline{x})| = 1$$

lie in the union of at most

$$12^n\, n^{4n}\, d^{n^2+n}$$

proper subspaces.

Note that for small solutions we did not need non-degeneracy or the hypothesis of Theorem 3B, but only the fact that the matrix of $L^{(1)}, \ldots, L^{(r)}$ is of rank n.

§9. Large Solutions.

We will count the large solutions only in the special case considered in Theorem 3B.

LEMMA 9A. *Let $L_1, \dots, L_n$ be n linearly independent linear forms in n variables with coefficients in a number field E. Using linear independence of $L_1, \dots, L_n$, write each variable as*

$$X_i = \gamma_{i1} L_1 + \ldots + \gamma_{in} L_n \qquad (i = 1, \dots, n)$$

with $\gamma_{ij} \in E$. Then

$$|\gamma_{ij}|\, |L_j| \leqq H_E(L_1) \ldots H_E(L_n). \qquad (i, j = 1, \dots, n)$$

Proof. In fact, for any absolute value $v^* \in M(E)$, we claim that

$$|\gamma_{ij}|_{v^*}\, |L_j|_{v^*} \leqq H_E(L_1) \ldots H_E(L_n).$$

Write

$$L_i(\underline{\underline{X}}) = \underline{\underline{\alpha}}_i \underline{\underline{X}} \qquad (i = 1, \dots, n)$$

and put

$$n'_v = \begin{cases} n_v \text{ if } v \neq v^*, \\ n_v - 1 \text{ if } v = v^*. \end{cases}$$

For $\alpha \in E^\times$, we have the product formula, namely

$$|\alpha|_{v^*} \prod_{v \in M(E)} |\alpha|_v^{n'_v} = 1.$$

Writing $\alpha = \det(\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_n)$, we get

$$\begin{aligned} \frac{1}{|\det(\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_n)|_{v^*}} &= \prod_{v \in M(E)} |\det(\underline{\underline{\alpha}}_1, \dots, \underline{\underline{\alpha}}_n)|_v^{n'_v} \\ &\leqq \prod_{v \in M(E)} (|\underline{\underline{\alpha}}_1|_v \cdots |\underline{\underline{\alpha}}_n|_v)^{n'_v} \qquad (9.1) \\ &= \frac{H_E(\underline{\underline{\alpha}}_1) \ldots H_E(\underline{\underline{\alpha}}_n)}{|\underline{\underline{\alpha}}_1|_{v^*} \cdots |\underline{\underline{\alpha}}_n|_{v^*}}, \end{aligned}$$

where we have used Hadamard's Inequality.

Now let $\underline{\underline{\alpha}}_i = (\alpha_{i1}, \dots, \alpha_{in})$, $A = (\alpha_{ij})$, $C = (\gamma_{ij})$. Then $AC = I$. Notice that the $\underline{\underline{\alpha}}_i$ are simply the rows of A, while $\underline{\underline{\gamma}}_j = \begin{pmatrix} \gamma_{1j} \\ \vdots \\ \gamma_{nj} \end{pmatrix}$ are the columns of C. Thus, up to sign,

$$\underline{\underline{\gamma}}_j = \frac{1}{\det A} \underline{\underline{\alpha}}_1 \wedge \ldots \wedge \underline{\underline{\alpha}}_{j-1} \wedge \underline{\underline{\alpha}}_{j+1} \wedge \ldots \wedge \underline{\underline{\alpha}}_n.$$

Now we have

$$|\underline{\underline{\alpha}}_j|_{v^*}\,|\underline{\underline{\gamma}}_j|_{v^*} \leqq \frac{|\underline{\underline{\alpha}}_1|_{v^*}\dots|\underline{\underline{\alpha}}_n|_{v^*}}{|\det A|_{v^*}} \leqq H_E(\underline{\underline{\alpha}}_1)\dots H_E(\underline{\underline{\alpha}}_n)$$

by (9.1). Looking at the ith components of the vectors $\underline{\underline{\gamma}}_j$ on the left, we have

$$|L_j|_{v^*}|\gamma_{ij}|_{v^*} \leqq H_E(\underline{\underline{\alpha}}_1)\dots H_E(\underline{\underline{\alpha}}_n),$$

as claimed.

Now suppose that $\underline{\underline{x}}$ is a solution of $F(\underline{\underline{x}}) = aL^{(1)}(\underline{\underline{x}})\dots L^{(n)}(\underline{\underline{x}}) = 1$.

LEMMA 9B. *If $\underline{\underline{x}}$ is a large solution in Theorem 3B, then there are indices $1 \leqq i_1 < \dots < i_n \leqq d$ such that*

$$|L^{(i_1)}(\underline{\underline{x}})\dots L^{(i_n)}(\underline{\underline{x}})| < |\det(L^{(i_1)},\dots,L^{(i_n)})|\,|\underline{\underline{x}}|^{-1/2}. \tag{9.2}$$

Proof. It is convenient to normalize the forms $L^{(i)}$. That is, let

$$M^{(i)}(\underline{\underline{X}}) = L^{(i)}(\underline{\underline{X}})\Big/|L^{(i)}|,$$

so that $|M^{(i)}| = 1$ $(i = 1,\dots,d)$. (Notice that the $M^{(i)}$ are no longer necessarily conjugate forms.) We have from $F(\underline{\underline{x}}) = 1$ that

$$|M^{(1)}(\underline{\underline{x}})\dots M^{(d)}(\underline{\underline{x}})| = \frac{1}{|a|\,|L^{(1)}|\dots|L^{(d)}|} = \frac{1}{H^*(F)} \leqq 1.$$

Without loss of generality,

$$|M^{(1)}(\underline{\underline{x}})| \leqq \dots \leqq |M^{(d)}(\underline{\underline{x}})|.$$

Since any n linear forms in Theorem 3B are linearly independent, we may express

$$X_i = \gamma_{i1}L^{(1)} + \dots + \gamma_{in}L^{(n)}.$$

Then by the preceding lemma,

$$|\gamma_{ij}|\,|L^{(j)}| \leqq H_E(L^{(1)})\dots H_E(L^{(n)}),$$

where E is a field containing all of the coefficients of $L^{(1)},\dots,L^{(n)}$. Then $\deg E \leqq d^n$, and

$$|\gamma_{ij}|\,|L^{(j)}| \leqq H(L)^{nd^n}.$$

Now express the variables X_i as linear combinations of $M^{(1)},\dots,M^{(n)}$, say

$$X_i = c_{i1}M^{(1)} + \dots + c_{in}M^{(n)},$$

where $c_{ij} = \gamma_{ij}|L^{(j)}|$. Then

$$|c_{ij}| \leqq H(L)^{nd^n}.$$

We can now obtain an estimate for $|\underline{x}|$, which we will use to complete the proof. We have

$$|\underline{x}| \leqq n^2 H(L)^{nd^n} |M^{(n)}(\underline{x})|.$$

Since

$$|M^{(1)}(\underline{x})| \leqq \dots \leqq |M^{(d)}(\underline{x})|,$$

the upper bound on $|\underline{x}|$ gives

$$|M^{(n+1)}(\underline{x}) \dots M^{(d)}(\underline{x})| \geqq \left(\frac{|\underline{x}|}{n^2 H(L)^{nd^n}}\right)^{d-n}.$$

Then

$$|M^{(1)}(\underline{x}) \dots M^{(d)}(\underline{x})| \leqq 1$$

leads to

$$|M^{(1)}(\underline{x}) \dots M^{(n)}(\underline{x})| \leqq \left(\frac{n^2 H(L)^{nd^n}}{|\underline{x}|}\right)^{d-n}.$$

Combining this last inequality with

$$|M^{(i)}(\underline{x})| = |L^{(i)}(\underline{x})| \Big/ |L^{(i)}|,$$

we have

$$\begin{aligned}\frac{|L^{(1)}(\underline{x}) \dots L^{(n)}(\underline{x})|}{|\det(L^{(1)}, \dots, L^{(n)})|} &\leqq \frac{|L^{(1)}| \dots |L^{(n)}|}{|\det(L^{(1)}, \dots, L^{(n)})|} \left(\frac{n^2 H(L)^{nd^n}}{|\underline{x}|}\right)^{d-n} \\ &< \left(\frac{n^2 H(L)^{2nd^n}}{|\underline{x}|}\right)^{d-n}\end{aligned}$$

since

$$\frac{|L^{(1)}| \dots |L^{(n)}|}{|\det(L^{(1)}, \dots, L^{(n)}|} < H(L)^{nd^n})$$

from the proof of the last lemma ((9.1) and the fact that $\deg E \leqq d^n$). Now, large solutions satisfy

$$|\underline{x}| > H(L)^{6nd^{n+1}} > n^{10dn},$$

(see the reduction of section 4), so

$$\begin{aligned}\frac{|L^{(1)}(\underline{x}) \dots L^{(n)}(\underline{x})|}{|\det(L^{(1)}, \dots, L^{(n)})|} &< \left(\frac{n^2}{|\underline{x}|^{2/3}}\right)^{d-n} \\ &< \left(\frac{1}{|\underline{x}|^{1/2}}\right)^{d-n} \leqq \frac{1}{|\underline{x}|^{1/2}}.\end{aligned}$$

Remark. We have not made full use of the restriction $|\underline{\underline{x}}| > H(L)^{6nd^{n+1}}$ for large solutions. Fuller use is made in the proof of Theorem 3A, which however is not presented here.

Now we apply the Subspace Theorem (Theorem 1D) with $\delta = 1/2$. The conclusion is that there exist subspaces $S_1, \dots , S_t$ where

$$t = \left[(2d^n)^{2^{26n}\delta^{-2}}\right] = (2d^n)^{4\cdot 2^{26n}},$$

such that solutions to (9.2) lie in the union of $S_1, \dots , S_t$ and the ball

$$|\underline{\underline{x}}| \leqq \max((n!)^{8/\delta},\ H(L)).$$

Since our large solutions can not lie in this ball, we have the following result.

PROPOSITION 9C. *Under the hypothesis of Theorem 3B, the large solutions to* $F(\underline{\underline{x}}) = 1$ *lie in the union of at most* t *proper subspaces, where*

$$t = (2d^n)^{4\cdot 2^{26n}}.$$

§10. Proof of Theorem 3B.

Combining the results of Sections 8 and 9 on small and large solutions, we see that the solutions to the norm form equation $F(\underline{\underline{x}}) = 1$ lie in the union of not more than

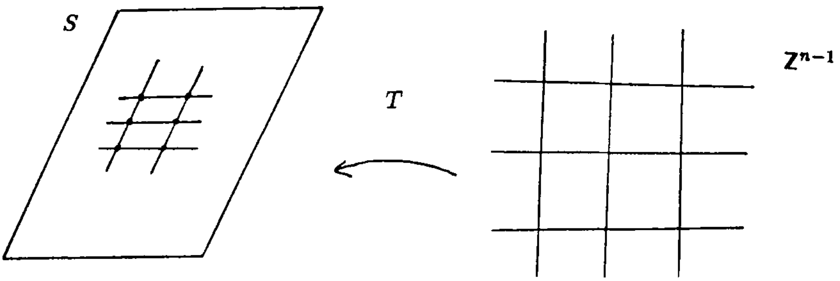
$$(2d^n)^{5\cdot 2^{26n}}$$

subspaces.

We want to count the number of solutions. We suppose that S is one of the subspaces and that S is given by a *parameter representation*

$$\underline{\underline{x}} = T\underline{\underline{y}},$$

where $\underline{\underline{y}} \in \mathbb{Q}^{n-1}$ and $T : \mathbb{Q}^{n-1} \to \mathbb{Q}^n$. If T is properly chosen, as $\underline{\underline{y}}$ runs through $\mathbb{Z}^{n-1}$, then $\underline{\underline{x}}$ will run through the integer points of S.



To study solutions $\underline{\underline{x}} \in S$, we need to study $F(T\underline{\underline{y}}) = 1$. Letting $L^*(\underline{\underline{y}}) = L(T(\underline{\underline{y}}))$, we have

$$aL^{*(1)}(\underline{\underline{y}}) \dots L^{*(d)}(\underline{\underline{y}}) = 1, \tag{10.1}$$

a norm form equation in $n-1$ variables. This allows us to do a proof by induction.

We would like to apply Theorem 3B to the new linear form L^*. By hypothesis, G was $n-1$ times transitive on $L^{(1)}, \dots, L^{(d)}$, so then G is $n-1$ times transitive, hence $n-2$ times transitive on $L^{*(1)}, \dots, L^{*(d)}$. Also, the rank of the forms $L^{*(1)}, \dots, L^{*(d)}$ is $n-1$. So then there exist $n-1$ among them which are linearly independent. By $(n-1)$-transitivity, any $n-1$ among them are linearly independent. So both hypotheses are satisfied, therefore (10.1) has

$$\leqq d^{2^{30(n-1)}}$$

solutions in S. Multiplying by the number of subspaces we get

$$\leqq d^{10n\cdot 2^{26n}} \cdot d^{2^{30(n-1)}} < d^{2^{30n}-10n^2}$$

solutions (with plenty to spare). This proves Proposition 4A, and therefore Theorem 3B.

Epilogue. The *abc*-conjecture.

Let a, b, c be non-zero integers with

$$a + b + c = 0 \quad \text{and} \quad gcd(a, b, c) = 1.$$

Put

$$P = \prod_{p|abc} p.$$

J. Oesterlé posed the following question. Is there an absolute constant c_1 such that

$$\max(|a|, |b|, |c|) \leqq P^{c_1} \ ?$$

Masser (1985) refined this question. He conjectured that for any $\epsilon > 0$, there exists a constant $c_2(\epsilon)$ such that

$$\max(|a|, |b|, |c|) < c_2(\epsilon)P^{1+\epsilon}.$$

This is known as the *abc*-conjecture. We will discuss consequences of the *abc*-conjecture. Our discussion will follow, to a large extent, a paper due to Stewart and Tijdeman (1986).

M. Hall Jr. (1971) conjectured that

$$|x^2 - y^3| > c_3 y^{1/2}$$

for positive integers x, y with $x^2 \neq y^3$. A weaker version of Hall's conjecture follows from the *abc*-conjecture. To see this, let $d = gcd(x^2, y^3)$, and then set $a = x^2/d$, $b = -y^3/d$, $c = (y^3 - x^2)/d$. Then

$$P = \prod_{p|abc} p \leqq \frac{xy|y^3 - x^2|}{d}.$$

The *abc*-conjecture gives for any $\epsilon > 0$ that

$$|b| = y^3/d < c_2(\epsilon)P^{1+\epsilon}$$

and

$$a = x^2/d < c_2(\epsilon)P^{1+\epsilon}.$$

Multiplying these inequalities, we get

$$\begin{aligned} x^2y^3/d^2 &< c_2(\epsilon)^2 P^{2+2\epsilon} \\ &< c_2(\epsilon)^2\, x^{2+2\epsilon}\, y^{2+2\epsilon}\, \frac{|y^3 - x^2|^{2+2\epsilon}}{d^{2+2\epsilon}}, \end{aligned}$$

and then

$$x^2\, y^3 < c_2\,(\epsilon)^2\, x^{2+2\epsilon}\, y^{2+2\epsilon}\, |y^3 - x^2|^{2+2\epsilon}.$$

Now we have

$$|x^2 - y^3|^{2+2\epsilon} > \frac{1}{c_2(\epsilon)^2}\, x^{-2\epsilon}\, y^{1-2\epsilon}.$$

If $x \leqq 2y^2$, then

$$|x^2 - y^3|^{2+2\epsilon} > c_4(\epsilon)\, y^{1-6\epsilon},$$

and therefore

$$|x^2 - y^3| > c_5(\epsilon)\, y^{(1-6\epsilon)/(2+2\epsilon)}.$$

So, again for every $\epsilon > 0$,

$$|x^2 - y^3| > c_6(\epsilon)\; y^{(1/2)-\epsilon}.$$

On the other hand, if $x > 2y^2$, we get

$$|x^2 - y^3| \geqq y^4.$$

So a weak form of Hall's conjecture follows, namely

$$|x^2 - y^3| > c_6(\epsilon)\, y^{(1/2)-\epsilon}.$$

This has the following consequence concerning a particular elliptic equation

$$y^2 = x^3 + k, \qquad k \neq 0,$$

called the *Mordell equation*. Hall's conjecture gives

$$|k| = |y^2 - x^3| > c_6(\epsilon) x^{(1/2)-\epsilon}.$$

Thus every solution to a given Mordell equation has

$$|x| < c_7(\epsilon)|k|^{2+\epsilon}.$$

Next we consider the Fermat conjecture. That is, we look at the equation

$$x^n + y^n = z^n$$

where

$$n \geqq 3, \quad gcd(x,y,z) = 1, \qquad \text{and} \quad x, y, z > 0.$$

To apply the *abc*-conjecture, let $a = x^n,\ b = y^n,\ c = -z^n$. Then

$$P = \prod_{p|abc} p \leqq xyz \leqq z^3,$$

since z is the largest of the three integers. By the *abc*-conjecture, we have

$$z^n = |c| \leqq c_2(\epsilon) P^{1+\epsilon} \leqq c_2(\epsilon) z^{3+3\epsilon},$$

so

$$z^{n-3-3\epsilon} \leqq c_2(\epsilon).$$

Now suppose that $n \geqq 4$ and $\epsilon < 1/3$. Since $n - 3 - 3\epsilon > 0$ in this case, we get a bound on z as well as a bound on n. Thus, for sufficiently large n, Fermat's conjecture is correct. In other words, Fermat is correct with at most finitely many exceptional n. And for any given n, there are still only finitely many solutions.

The weaker Oesterlé conjecture also has this consequence about the Fermat Conjecture. However, in that case, we obtain a larger lower bound on n, so we get more possible exceptions. We then also need Falting's Theorem (1983) to deal with small n.

The following conjecture was made by Pillai (1945). Given integers $A > 0$, $B > 0$, $C > 0$, the equation

$$Ax^n - By^m = C$$

in integers $x > 1, y > 1, n > 1, m > 1$ and with $(m,n) \neq (2,2)$ has only a finite number of solutions. If m, n were fixed, this would be a special case of an algebraic diophantine equation, the superelliptic equation. The conjecture has been proved only for $A = B = C = 1$, by Tijdeman (1976). This special case

$$x^n - y^m = 1$$

ties in with Catalan's conjecture, namely that this equation has no solutions except $3^2 - 2^3 = 1$. Tijdeman showed that all solutions have $x, y, m, n \leqq B$ for some explicit B.

To apply the *abc*-conjecture to Pillai's conjecture, let $d = gcd(Ax^n,\ By^m,\ C)$. Set $a = Ax^n/d$, $b = -By^m/d$, and $c = -C/d$. Then

$$P \leqq ABCxy,$$

and the *abc*-conjecture gives

$$Ax^n/d,\ By^m/d \leqq c_2(\epsilon)P^{1+\epsilon}.$$

So

$$\max(x^n, y^m) \leqq c_8(A,B,C,\epsilon)(xy)^{1+\epsilon}.$$

Without loss of generality, $x^n \leqq y^m$, so

$$y^m \leqq c_8\,(A,B,C,\epsilon)y^{(1+(m/n))(1+\epsilon)}.$$

If $m \geqq 3$, then $1 + (m/n) \leqq 1 + (m/2) \leqq \frac{5}{6}m$, so $(1 + (m/n))(1 + \epsilon) < \frac{6}{7}m$ for $\epsilon > 0$ sufficiently small. Then

$$y^{m/2} < y^{m-(1+(m/n))(1+\epsilon)} < c_8(A,B,C,\epsilon)$$

gives an upper bound for y^m, hence for y and for m. On the other hand, if $m = 2$, then $n \geqq 3$ and $(1 + (m/n)) \leqq 1 + (m/3) \leqq \frac{5}{6}m$, and the rest follows as before.

A more general application is as follows. Tijdeman (1989) proved that for given non-zero integers A, B, C the diophantine equation

$$Ax^n + By^m = Cz^\ell$$

has only finitely many solutions in positive integers $x > 1$, $y > 1$, $z > 1$, n, m, ℓ subject to $gcd(Ax, By, Cz) = 1$ and $n^{-1}+m^{-1}+\ell^{-1} < 1$. On the other hand, Hindry has shown that for each triple n, m, ℓ with $n^{-1}+m^{-1}+\ell^{-1} \geqq 1$, there exist A, B, C such that the above equation has infinitely many solutions x, y, z with g.c.d. $(Ax, By, Cz) = 1$.

Last, we consider S-unit equations over $\mathbb{Q}$. Let $K = \mathbb{Q}$ and $S = \{\infty, p_1, \dots, p_\nu\}$. Consider the equation

$$x + y + z = 0,$$

where

$$x, y, z \in U_S \cap \mathbb{Z} \quad \text{and} \quad gcd(x, y, z) = 1.$$

To apply the abc-conjecture, let $a = x$, $b = y$, $c = z$. Then

$$P \leqq p_1 \dots p_\nu$$

and

$$|x|,\ |y|,\ |z| \leqq c_2(\epsilon)P^{1+\epsilon}$$

The abc-conjecture may be an elusive goal. What do we know in this direction?

THEOREM 1. (Stewart and Yu, (to appear)). *Under the hypothesis of the abc-conjecture,*

$$\max(|a|,\ |b|,\ |c|) < e^{P^{2/3}+c_9/\log\log P}.$$

This improves upon an earlier bound due to Stewart and Tijdeman (1986)).

THEOREM 2. (Stewart and Tijdeman, 1986). *In this setting the conjecture would be false without the ϵ. In other words, it is not true that*

$$|a|,\ |b|,\ |c| < c_{10}P.$$

More precisely, given $\delta > 0$, there are infinitely many positive integers a, b, c with $gcd(a, b, c) = 1$ and $a = b + c$ such that

$$a > Pe^{(4-\delta)\frac{\sqrt{\log P}}{\log\log P}},$$

where $P \prod_{p|abc} p$.

We have the following generalization to n variables. Suppose

$$a_1 + a_2 + \dots + a_n = 0,$$

where the a_i are non-zero integers, $gcd(a_i,\ a_j) = 1$ for $i \neq j$, and no sub-sum vanishes. Let

$$P = \prod_{P|a_1\dots a_n} p.$$

The conjecture is that

$$\max(|a_1|, \dots, |a_n|) < c_{11}(n, \epsilon)P^{n-2+\epsilon}.$$

Bibliography

A. Baker (1964). *Rational Approximations to certain algebraic numbers.* Proc. London Math. Soc. 4, 385–398.

A. Baker (1968). *Contributions to the theory of diophantine equations.* Phil. Trans. Roy. Soc. London A263, 173–208.

A. Baker and J. Coates (1970). *Integer points on curves of genus 1.* Proc. Camb. Phil. Soc. 68, 105–123.

A. Baker and C. L. Stewart (1988). *On effective approximations to cubic irrationals.* New Advances in Transcendence Theory (Ed. by A. Baker). Camb. Univ. Press.

H. F. Blichfeldt (1929). *The minimum value of quadratic forms and the closest packing of spheres.* Math. Ann. 101, 665–608.

E. Bombieri (1982). *On the Thue–Siegel–Dyson Theorem.* Acta Math. 148, 255–296.

E. Bombieri (1985). *On the Thue-Mahler equation.* (Diophantine approximation and transcendence theory. Bonn 1985) Springer Lecture Notes 1290, 213-243.

E. Bombieri. The Mordell Conjecture Revisited. (to appear).

E. Bombieri and J. Mueller (1983). *On effective measures of irrationality for* $\sqrt[3]{(a/b)}$ *and related numbers.* J. reine angew. Math. 342, 173–196.

E. Bombieri and W. M. Schmidt (1987). *On Thue's equation.* Inv. Math. 88, 69–81.

E. Bombieri and J. Vaaler (1983). *On Siegel's Lemma.* Invent. Math. 73, 11–32.

E. Bombieri and A. J. Van der Poorten (1988). *Some quantitative results related to Roth's theorem.* J. Austral. Math. Soc. (Series A) 45, 233-248.

Z. I. Borevich and I. R. Shafarevich (1966). *Number Theory.* Academic Press. (Translated from 1964 Russian edition).

J. W. S. Cassels (1957). *An introduction to diophantine approximation.* Cambridge Tracts 45, Cambridge Univ. Press.

J. W. S. Cassels (1959). *An introduction to the Geometry of Numbers.* Springer Grundlehern 99. Berlin–Göttinger–Heidelberg.

S. Chowla (1933). *Contributions to the analytic theory of numbers (II).* J. Indian Math. Soc. 20, 120-128.

G. V. Chudnovsky (1983). *On the method of Thue–Siegel.* Ann. Math. 117, 325–382.

H. Davenport and K. F. Roth (1956). *Rational approximations to algebraic numbers.* Mathematika 2, 160–167.

V. A. Dem'janenko (1974). *On Tate height and the representation of a number by binary forms.* Math. USSR Izv. 8, 463-476.

M. Deuring (1973). *Lectures on the Theory of Algebraic Functions of One Variable.* Springer Lecture Notes 314.

L. G. P. Dirichlet (1842). *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen.* S. B. Preuss. Akad. Wiss., 93–95.

Y. Domar (1954). *On the diophantine equation* $|Ax^n - By^n| = 1$, $n \geqq 5$. Math. Scand. 2, 29–32.

E. Dubois and G. Rhin (1976). *Sur la majoration de formes linéares à coefficients algébriques réels et p-adiques. Demonstration d' une conjecture de K. Mahler.* C.R. Acad. Sci. Paris 282, Série A, 1211

F. J. Dyson (1947). *The approximation to algebraic numbers by rationals.* Acta Math. Acad. Sci. Hung. 9, 225–240.

P. Erdös, C. L. Stewart and R. Tijdeman (1988). *Some diophantine equations with many solutions.* Compositio Math. 66, 37-56

P. Erdös and P. Turan (1950). *On the distributions of roots of polynomials.* Ann. of Math. **(2)** 51, 105-119.

H. Esnault and E. Viehweg (1984). *Dyson's Lemma for polynomials in several variables (and the theorem of Roth).* Invent. Math. 78, 445–490.

J. H. Evertse (1982). *On the equation* $ax^n - by^n = c$. Compositio Math. 47, 288–315.

J. H. Evertse (1983). *Upper bounds for the numbers of solutions of Diophantine equations.* Math Centrum tract 168, pp. 1–127, Amsterdam.

J. Evertse (1984a). *On equations in S-units and the Thue-Mahler equation.* Invent. Math. 75, 561–584.

J. H. Evertse (1984b). *On sums of S-units and linear recurrences*, Comp. Math. 53, 225–244.

J. H. Evertse, K. Györy, C. L. Stewart and R. Tijdeman (1988). *S-unit equations and their applications.* New Advances in Transcendence Theory. Camb. Univ. Press 110-174.

J. H. Evertse and J. H. Silverman. (1986) *Uniform bounds for the number of solutions to* $Y^n = f(X)$. Math. Proc. Camb. Phil. Soc. 100, 237-248.

G. Faltings (1983). *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73, 349-366.

N. I. Feldman (1971). *An effective refinement of the exponent in Liouville's theorem* (in Russian). Izv. Akad. Nauk. SSSR 35, 973–990.

A. O. Gelfond (1952). *Transcendental and Algebraic Numbers.* (Russian). English transl. (1969), Dover Publications, New York.

P. M. Gruber and C. G. Lekkerkerker (1987). *Geometry of Numbers.* Second edition, North–Holland Mathematical Library, vol. 37.

M. Hall Jr. (1971). *The diophantine equation* $x^3 - y^2 = k$. In: Computers in Number Theory, A.O. Atkin and B.J. Birch (eds.). Proc. Sci. Res. Council Atlas Symp. No. 2, Oxford, 1969, pp. 173-198. London: Academic Press.

G. Hardy and E. M. Wright (1954). *An introduction to the theory of numbers.* 3rd ed. Oxford, Clarendon Press.

A. Hurwitz (1891). *Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche.* Math Ann. 39, 279–284.

S. Hyyrö (1964). *Über die Gleichung* $ax^n - by^n = c$ *und das Catalansche Problem.* Ann. Acad. Sci. Fenn Ser. AI, 355, 1–50.

G.A. Kabatjanskii and V.I. Levenšteĭn (1978). *Bounds for packings on the sphere and in space.* (in Russian). Problemy Peredači Informacii 14, 3-25

A. Khintchine (1926). *Zur metrischen Theorie der diophantischen Approximationen.* Math. Z. 24, 706–714.

N. Koblitz (1977). *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Springer Graduate Texts 58.

A. G. Khovansky (1981). *Sur les racines complexes des systèmes d'équations algébriqeus comportant peu de termes.* C.R. Acad. Sci. Paris 292, 937-940.

S. Lang (1962). *Diophantine Geometry.* Interscience Publishers.

D. J. Lewis and K. Mahler (1961). *On the representation of integers by binary forms.* Acta Arith. 6, 333–363.

J. Liouville (1844). *Sur des classes très-étendues de quantités dont la irrationelles algébriques.* C. R. Acad. Sci. Paris 18, 883–885 and 910–911.

H. Luckhardt (1989). *Herbrand-Analysen zweier Beweise des Satzes von Roth: polynomiale Anzahlschranken*, The Journal of Symbolic Logic, **54** no. 1, 234-263.

K. Mahler (1933). *Zur Approximation algebraischer Zahlen I. Über den grössten Primteiler binärer Formen.* Math Ann. 107, 691-730.

K. Mahler (1934). *Zur Approximation algebraischer Zahlen. III.* Acta Math. 62, 91-166.

K. Mahler (1935). *On the lattice points on curves of genus 1.* Proc. London Math. Soc. (**2**) 39, 431-466.

D. W. Masser (1985). *Open problems.* Proc. Symp. Analytic Number Th., W.W.L. Chen (ed). London: Imperial College.

H. Minkowski (1896 & 1910). *Geometrie der Zahlen.* Teubner: Leipzig u. Berlin. (The 1910 ed. prepared posthumously by Hilbert and Speiser).

L. J. Mordell (1922). *Note on the integer solutions of the equation $Ey^2 = Ax^3 + Bx^2 + Cx + D$.* Messenger Math. 51, 169-171.

L. J. Mordell (1922). *On the rational solutions of the indeterminate equations of the third and fourth degrees.* Proc. Camb. Phil. Soc. 21, 179-192.

L. J. Mordell (1934). *On some arithmetical results in the geometry of numbers.* Compositio Math. 1, 248–253.

J. Mueller (1987). *Counting solutions of $|ax^r - by^r| \leqq h$.* Quarterly J. Oxford (2) 32, 503–513.

J. Mueller and W. M. Schmidt (1987). *Trinomial Thue equations and inequalities.* J. reine aug. Math. 379, 76–99

_______________ (1988). *Thue's equation and a conjecture of Siegel.* Acta Math. 160, 207–247.

_______________ (1989). *On the number of good rational approximations to algebraic numbers.* Proc. A.M.S. 106, 859-866.

T. Nagell (1969). *Quelques problèmes relatifs aux unités algébriques.* Ark. Mat. 8, 115-127.

A. Ostrowski (1935). *Untersuchungen zur arithmetischen Theorie der Kőrper.* Math. Zeit. 39, 269–404.

S. S. Pillai (1945). *On the equation $2^x - 3^y = 2^X + 3^Y$.* Bull. Calcutta Math. Soc. 37, 15-20.

K. Ramachandra (1969). *A lattice point problem for norm forms in several variables.* J. Number Theory 1, 534-555.

D. Ridout (1958). *The p-adic generalization of the Thue–Siegel–Roth Theorem.* Mathematika 5, 40–48.

J. Risler (1984/85). *Complexité et Géométrie Réelle.* Sém. Bourbaki, no. 637, 89-100.

C. A. Rogers (1964). *Packing and Covering.* Cambridge Tracts in Math. and Math. Phys. 54.

K. F. Roth (1955). *Rational approximations to algebraic numbers.* Mathematika 2, 1–20.

S. Schanuel (1979). *Heights in number fields.* Bull. Soc. Math. France 107, 433–449.

H. P. Schlickewei (1977a). *The p-adic Thue-Siegel-Roth-Schmidt theorem.* Arch. Math. 29, 267-270.

H. P. Schlickewei (1977b). *Über die diophantische Gleichung* $x_1 + x_2 + \ldots + x_n = 0$. Acta. Arith. 33, 183-185.

H. P. Schlickewei (to appear (a)). *The number of subspaces occurring in the p-adic subspace theorem in diophantine approximation.* J. f. d. reine und. ang. Math.

H. P. Schlickewei (to appear (b)). *The quantitative subspace theorem for number fields.*

H. P. Schlickewei (to appear (c)). *An explicit upper bound for the number of solutions of the S-unit equation.*

H. P. Schlickewei (to appear (d)). *S-unit equations over number fields.*

H. P. Schlickewei and A. J. Van der Poorten (1982). *The growth conditions for recurrence sequences.* Macquarie Univ. Math. Rep. 82-0041. North Ryde, Australia.

W. M. Schmidt (1967). *On heights of subspaces and diophantine approximations.* Annals of Math. 85, 430–472.

W. M. Schmidt (1968). *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height.* Duke Math. J. 35, 327–339.

W. M. Schmidt (1972). *Norm form equations.* Ann. of Math. 96, 526-551.

W. M. Schmidt (1980). *Diophantine approximation.* Springer Lecture Notes in Mathematics 785.

W. M. Schmidt (1985). *Small zeros of quadratic forms.* Trans. AMS 291, 87–102.

W. M. Schmidt (1987). *Thue equations with few coefficients.* Transactions A.M.S. 303, 241–255.

W. M. Schmidt (1989a). *The Subspace Theorem in diophantine approximations.* Compositio Math. 69, 121–173.

W. M. Schmidt (1989b). *The number of solutions of norm form equations.* Transactions A.M.S. 317, 197–227.

W. M. Schmidt. *Integer points on curves of genus 1.* Compositio Math. (to appear).

T. N. Shorey and R. Tijdeman (1986). *Exponential diophantine equations.* Cambridge Univ. Press.

C. L. Siegel (1921). *Approximation algebraischer Zahlen.* Math. Zeitschr. 10, 173–213.

C. L. Siegel (1926). *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$. J. London Math. Soc. 1, 66-68.

C. L. Siegel (1929). *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. d. Wiss., Math. Phys. Kl., Nr. 1 = Ges. Abh. I, 209–266.

C. L. Siegel (1970). *Einige Erläuterungen zu Thues Untersuchungen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen.* Nachr. Akad. Wiss. Göttingen, Math. phys. Kl. Nr. 8, 169-195.

J. H. Silverman (1981). *Lower bound for the canonical height on elliptic curves.* Duke Math. J. 48, 633-648.

J. H. Silverman (1982). *Integer points and the rank of Thue elliptic curves.* Invent. Math. 66, 395-404.

J. H. Silverman (1983). *Integer points on curves of genus 1.* J. London Math. Soc. **(2)** 28, 1-7.

J. H. Silverman (1985). *The Arithmetic of Elliptic Curves.* Springer Graduate Texts in Mathematics 106.

N. Stephens (1968). *The Diophantine equation* $x^3 + y^3 = Dz^3$ *and the conjectures of Birch and Swinnerton-Dyer.* J. Reine Angew. Math. 231, 121-162.

C. L. Stewart (to appear). *On the number of solutions of polynomial congruences and Thue equations.*

C. L. Stewart and R. Tijdeman (1986). *On the Oesterlé-Masser Conjecture.* Monatsh. Math. 102, 251-257.

A. Thue (1892). *Om nogle geometrisk-taltheoretiske*, Theoremer, Forhandl. ved de Skand. Naturforskeres 14, 352–353, in Danish; Über die dichteste Zusammenstellung von Kreisen in einer Ebene, *Skr. Vidensk.-Selsk.*, Christ. 1 (1919), 1–9.

A. Thue (1909). *Über Annäherungswerte algebraischer Zahlen.* J. reine angew. Math. 135, 284–305.

J. Thunder (to appear). *Asymptotic formulae for the number of subspaces of bounded height over number fields.*

R. Tijdeman (1976). *On the equation of Catalan.* Acta Arith. 29, 197-209.

R. Tijdeman (1989). *In Number Theory and Applications*, ed. by R. A. Mollin, Kluwer, p. 234.

J. Vaaler (1979). *A geometric inequality with applications to linear forms.* Pacific J. 83, 543–553.

C. Viola (1985). *On Dyson's Lemma.* Ann. Sc. Norm. Sup. Pisa, Classe di Sc. IV, 12, 105–135.

P. Vojta (to appear). *Siegel's theorem in the compact case.* Annals of Math.

H. Zimmer (1976). *On the difference of the Weil height and Néron-Tate height.* Math Zeit. 147, 35-51.

Index of some definitions